KPMG

Vientos de cambio

La gestión de riesgos en el mundo digital

Riesgos

Febrero 2019

kpmg.es

Índice

La gestión de riesgos en el mundo digital

Prólogo

Hace ahora diez años, iniciamos desde KPMG una aproximación integral y coordinada al mundo de la gestión de riesgos empresariales. Previo a ese momento, identificamos que los riesgos tenían naturaleza individual y estaban relativamente aislados unos de otros. La velocidad del cambio, la transformación digital, el entorno regulatorio, la creciente presión pública y un nivel de incertidumbre en ascenso han hecho que los riesgos estén ahora conectados, tengan mayores implicaciones y sean mucho más difíciles de gestionar que en el pasado. La revolución tecnológica sin duda conlleva la aparición de nuevos riesgos, pero al mismo tiempo nos brinda increíbles posibilidades para monitorizar y prevenir las consecuencias de los mismos.

En este nuevo entorno de disrupción tecnológica, me complace presentarles el primer informe transversal que hemos realizado desde el área de Consultoría de Riesgos de KPMG en España, con el objetivo de poner de manifiesto no solo la creciente complejidad e interrelación de los riesgos a los que tienen que hacer frente las empresas, sino también algo que corre paralelo a este nuevo escenario: la cada vez mayor importancia de la función de gestión de riesgos y su progresiva digitalización.

La gestión de riesgos es hoy una palanca crítica en las empresas, que tienen que lidiar con un mundo de cambio constante y en el que la agilidad es clave para sobrevivir. La gestión de riesgos está –o debe estar- conectada al *core business*, al negocio, y complemente integrada en la estrategia empresarial.

Además de adquirir este protagonismo, la función de la gestión de riesgos no está siendo ajena al proceso de digitalización. Coincidirán conmigo en que nos encontramos en un momento sin precedentes. Un momento en el que la innovación tecnológica y digital está cambiando completamente la sociedad, la forma en que trabajamos, vivimos, compramos, nos relacionamos… Un nuevo contexto que nos exige adaptarnos. La transformación ya no es algo opcional. Es una imperiosa necesidad. No se puede vivir al margen de la tecnología, máxime cuando la tecnología está ahí precisamente para ayudarnos a mejorar nuestra vida, nuestra sociedad, pero también las tareas y procesos empresariales, como es el caso que nos ocupa.

Los métodos tradicionales de medición y control de riesgos, centrados fundamentalmente en dos variables, impacto y probabilidad, no son suficientes ahora para poder anticiparse. Los métodos convencionales miran al pasado. En un mundo de cambio constante como el actual, hay que estar preparado tanto para lo probable o posible, como para lo improbable o imposible. No basta con analizar lo ya conocido. Y es en esa tarea en la que la tecnología resulta no solo oportuna sino crítica.

Técnicas como *Big Data Analytics, Machine Learning, Blockchain* o Inteligencia Artificial, que ya están utilizando algunas empresas y hasta supervisores -sobre todo de mercados- nos permiten analizar ingentes volúmenes de datos para llevar a cabo una gestión más ágil, precisa y predictiva de los riesgos. Ya sea fraude, ciberseguridad, riesgos de gobernanza, de complimiento normativo, financieros, reputacionales, legales o cualquier otra variante de las que analizamos en este informe. La tecnología, si está bien parametrizada, permite hacer una gestión de riesgos consolidada y totalmente granulada al mismo tiempo, y prácticamente en tiempo real, lo que posibilita reaccionar con agilidad y aportar más valor al negocio. En definitiva, una gestión de riesgos que de verdad esté a la altura de los retos que exige el mundo de los negocios en la era digital.

Pablo Bernad
Socio responsable de Consultoría de Riesgos de KPMG en España

KPMG

La gestión de riesgos en el mundo digital

La gestión de riesgos como estrategia

En un mundo de cambio constante, es imposible tener visibilidad a largo plazo y la gestión de riesgos se vuelve crítica.

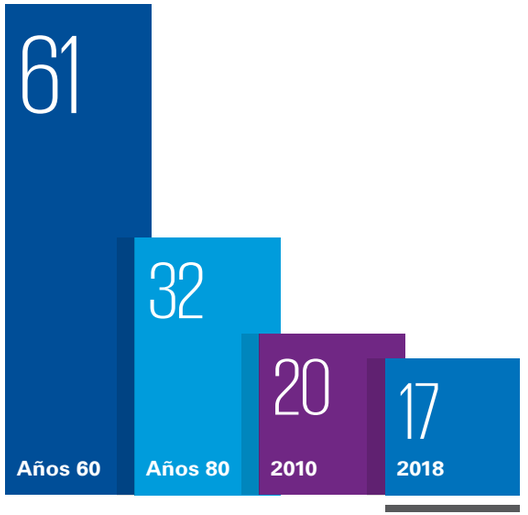
Históricamente, la gestión de riesgos ha estado muy enfocada al cumplimiento normativo y al reporte financiero. Predominaba la cultura de evitar los riesgos más que gestionarlos. Una actitud defensiva más que proactiva.

Hoy eso es imposible en un mundo en el que los cambios, impulsados por la revolución tecnológica y digital, se suceden a una velocidad de vértigo. Surgen tecnologías disruptivas. Nuevos canales de distribución. Nuevas regulaciones. La digitalización de las cosas se suma a la de las personas. Cambian los hábitos de los consumidores. Aparecen nuevos desafíos demográficos. Los *stakeholders* son cada vez más numerosos y exigentes. La geopolítica adquiere gran volatilidad. Se borran las fronteras entre geografías y sectores. Surgen nuevos y complejos riesgos, más dinámicos e interconectados, porque la digitalización magnifica los riesgos. En este entorno de cambio constante es muy difícil tener visibilidad sobre el medio y el largo plazo, el horizonte natural sobre el que durante décadas ha discurrido la estrategia empresarial, y la gestión de riesgos cobra gran relevancia en un mundo en el que la agilidad es crítica para sobrevivir.

Impulsada por factores internos y externos –especialmente reguladores e inversores- la gestión de riesgos ha dejado de ser la vieja función periférica y dispersa entre varios departamentos para adquirir identidad propia como disciplina. Aparece cada vez más conectada al *core business*, al negocio, y está completamente integrada en la estrategia empresarial. Se diría incluso que es la única estrategia posible en la era del cambio constante.

Gráfico 1

La vida media de las empresas del índice S&P 500



Fuente: Richard Foster, profesor de la Universidad de Yale y autor del libro "Creative Destruction"

La gestión de riesgos en el mundo digital

Gráfico 2

La velocidad de la innovación

El mundo ha pasado de ser plano y previsible a muy volátil debido a la globalización y a la rápida adopción de las nuevas tecnologías

La gestión de riesgos en el mundo digital

La relevancia de la función de riesgos ha quedado patente con la aparición de la figura del *Chief Risk Officer* y, especialmente, con la implicación directa del consejo de administración al atribuirle como una de sus "facultades indelegables" la determinación y supervisión de la política de control y gestión de riesgos de las organizaciones. Como órgano supervisor, el consejo debe, entre otros aspectos, aprobar el nivel del apetito al riesgo considerado aceptable para la organización y asegurarse de que la sociedad dispone de una función de control y gestión de riesgos eficaz ejercida por una unidad interna, bajo la supervisión directa de la Comisión de Auditoría o, en su caso, de una comisión especializada del consejo [(1)].

Aunque en este aspecto se ha avanzado mucho en los últimos años, quedan aspectos por mejorar a los ojos de los supervisores. "La involucración de la función de riesgos en el proceso de fijación de límites es aún pobre y poco ambiciosa. Las funciones de control interno tienen que fortalecerse, especialmente en riesgos y compliance", decía Margarita Delgado, subgobernadora del Banco de España (BdE), en el IX Encuentro Financiero Expansión-KPMG [(2)].

La tecnología acelera la transformación de la función

El proceso de transformación de la función de riesgos está dando un paso más allá con la utilización de nuevas metodologías. Los métodos tradicionales de medición y control de riesgos, centrados fundamentalmente en dos variables, impacto y probabilidad, no son suficientes para poder anticiparse. Los métodos convencionales miran al pasado. Pero los riesgos, antes de su manifestación, son desconocidos e imprevisibles y cada día más complejos y devastadores. Hay muchos ejemplos de compañías que han perdido valor o incluso han desaparecido por inadecuadas políticas de gestión de riesgos.

Para gestionar los riesgos en este entorno de cambio es imprescindible conocer las fuerzas visibles e invisibles que los mueven; todas las variables que inciden o podrían incidir en ellos; identificar el grado de interrelación real o potencial y la velocidad a la que se propagan en solitario o conjuntamente. Y, por supuesto, llevar a cabo una gestión, no fragmentada como en el pasado, sino consolidada y agregada, aunque también lo más granulada y segmentada posible, de todos los riesgos que afectan o pueden afectar al negocio.

Todo esto solo es posible hoy en día con el apoyo de las tecnologías emergentes y disruptivas como *Big Data Analytics, Machine Learning* o Inteligencia Artificial, que permiten analizar ingentes volúmenes de datos –algo antes imposible– para llevar a cabo una gestión más ágil, precisa y predictiva, de los riesgos. Una gestión en tiempo real, que aporte más valor al negocio. Es lo que realmente requieren las organizaciones para estar a la altura de los retos del siglo XXI.

La función de gestión de riesgos ha adquirido su propia identidad y peso en la estrategia empresarial

La gestión de riesgos en el mundo digital

La figura del CRO

La profesionalización de la gestión de riesgos ha venido de la mano de la emergente figura del *Chief Risk Officer* (CRO). Se trata de una posición cada día más común –aunque predomina en el sector financiero más que en otros – que muestra la creciente importancia de la función de gestión de riesgos. Ésta nació ligada a la función financiera pero va adoptando su propia identidad y cobrando peso en las organizaciones. El primer CRO del mundo lo nombró GE Capital en 1993. La figura se ha visto impulsada tras la crisis financiera de 2008. Los CRO tienen línea directa con los máximos ejecutivos y una relación muy fluida con el resto de los órganos de gobierno de la empresa, especialmente con el consejo de administración.

La gestión de riesgos del siglo XXI requiere contar con nuevas tecnologías que permitan un análisis en tiempo real

Los riesgos son cada vez más dinámicos y devastadores y exigen agilidad empresarial para sobrevivir

El efecto cascada

Lo que actualmente complica la gestión de riesgos es que, a diferencia del pasado, que casi podían gestionarse individualmente, hoy los riesgos son más numerosos, menos previsibles e interactúan entre ellos generando una maraña de nuevos escenarios e implicaciones. A continuación mostramos un ejemplo del efecto cascada que, por ejemplo, puede generar una brecha de seguridad.

Digitalización de la función de riesgos

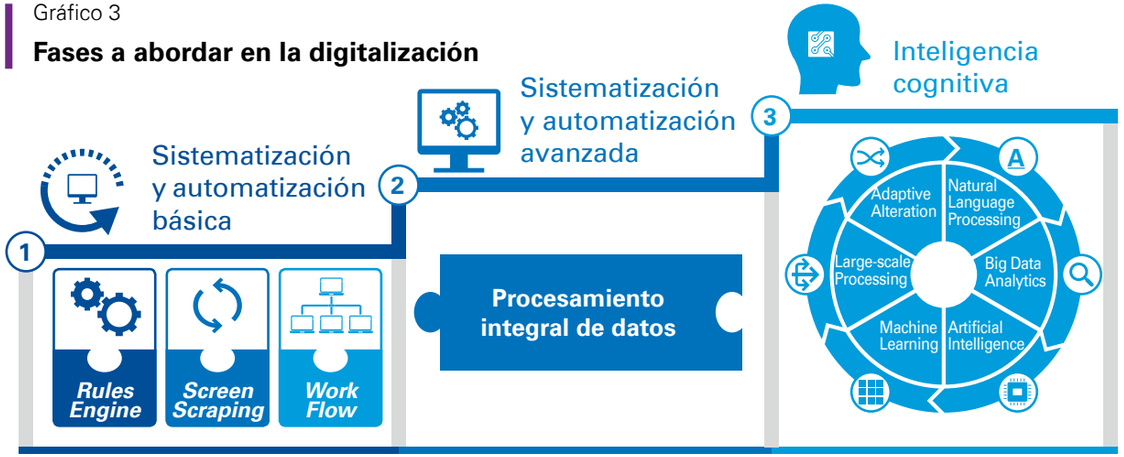
No tiene sentido una gestión de riesgos analógica en un mundo cada vez más digital.

La digitalización de la función de riesgos es un fenómeno tan reciente como apremiante. El sector financiero, y los riesgos financieros propiamente dichos, van por delante abriendo camino en este proceso de digitalización, como veremos más adelante.

Las empresas, que inicialmente abrazaron las tecnologías disruptivas como *Big Data Analytics, Machine* y *Deep Learning* o Inteligencia Artificial, para adaptar los procesos del *front-office* y mejorar la experiencia de clientes, están abordando ahora a los procesos de *back-office*. Uno de ellos es la función de riesgos. Su digitalización, que habitualmente sigue una hoja de ruta, mejora la eficacia de la función y la calidad de las decisiones.

Gráfico 3

Fases a abordar en la digitalización



- Programación basada en macros.
- Captura de información de las pantallas.
- Flujogramas de trabajo.
- Sistematización de los procesos.
- Gestión de procesos de negocio.

- Capacidad de trabajar con información desestructurada.
- Reconocimiento de patrones.
- Analítica avanzada.
- Modelos 3.0.
- Ingesta de datos masiva.

- Reconocimiento y procesamiento de lenguaje natural.
- Auto optimización y auto aprendizaje.
- Análisis de grandes cantidades de datos.
- Analítica predictiva y generación de hipótesis.
- Aprendizaje basado en las evidencias.
- Inteligencia artificial.

Fuente: KPMG en España

La gestión de riesgos en el mundo digital

Las ventajas que estas tecnologías –a las que en el futuro se unirán Blockchain y otras que lleguen- aportan a la función de riesgos son múltiples y variadas: desde una monitorización más sofisticada y precisa, con visión consolidada y prácticamente en tiempo real (24:7); capacidad de responder rápidamente ante cualquier evento e incluso anticiparse con análisis predictivos; análisis tan afinados que permiten desarrollar nuevos productos, servicios y hasta personalizaciones antes impensables; aportación de más valor a la compañía, que ve reforzada su capacidad de resiliencia, y un largo abanico de oportunidades.

La digitalización de la función de gestión de riesgos hará que sea más precisa y ágil

Gráfico 4

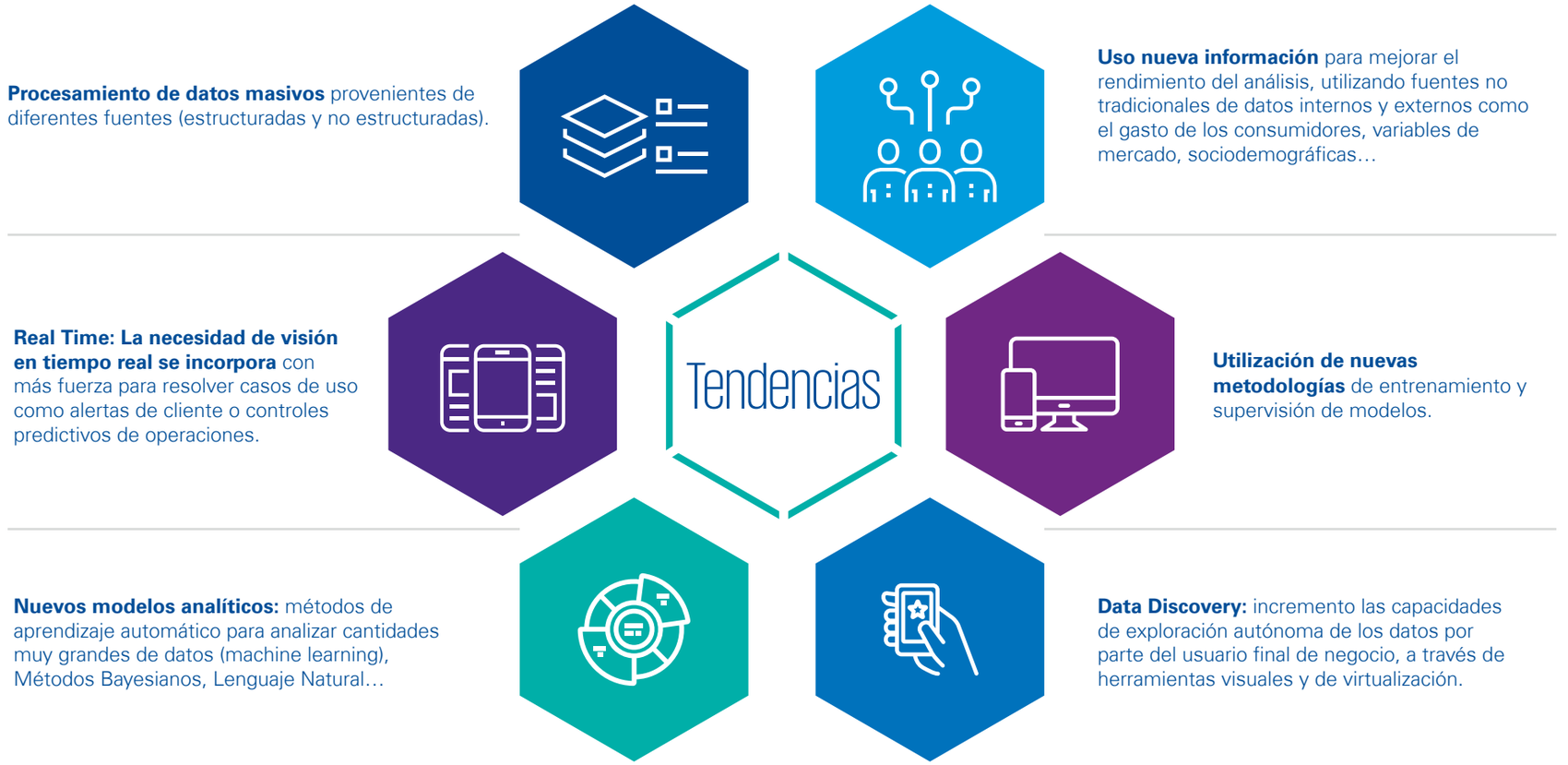
Beneficios de la digitalización de la función de riesgos

Fuente: KPMG en España

La gestión de riesgos en el mundo digital

Gráfico 5

Capacidades analíticas necesarias



Fuente: KPMG en España

La gestión de riesgos en el mundo digital

¿De qué tecnologías estamos hablando y cómo se aplican a la gestión de riesgos? Básicamente de todas las que tienen que ver con la captación y análisis de datos, tanto datos tradicionales o estructurados como no estructurados –*Big Data Analytics*, *Machine Learning* e Inteligencia Artificial – y con la automatización y gestión de procesos y tareas –*Workflow Automation (iBPM)* y *Robotic Process Automation (RPA)*–.

Las primeras, especialmente Inteligencia Artificial, son las que están llamadas a aportar un enorme potencial a la función de riesgos y las últimas juegan un papel relevante para mejorar la eficiencia de los procesos y tareas manuales, tremendamente rutinarias o repetitivas, en las que la intervención humana puede derivar en errores.

Expliquemos brevemente en qué consisten.

Workflow Automation (iBPM)

Son como los *project plans*, flujogramas de trabajo u orquestadores automáticos de las actividades. Permiten un mayor control y monitorización al conocer en tiempo real el estado de situación de los diferentes procesos intervinientes: qué se ha hecho, con qué resultado y qué queda por hacer.

Robotic Process Automation (RPA)

Automatización de procesos y tareas. Los conocidos *bots* que hacen una réplica automática de las tareas del usuario. Permiten liberar recursos humanos para dedicarlos a tareas de más valor añadido.

Big Data & Analytics

Mucho más sofisticada que la analítica que durante décadas se ha utilizado en los bancos. Permite gestionar ingentes volúmenes de datos y buscar correlaciones y patrones de comportamiento así como modelizar diferentes riesgos.

Machine Learning y Deep Learning

Al margen de la discusión de si es una variante de Inteligencia Artificial o no, permiten a las máquinas aprender de la experiencia, de su propio análisis y de los imputs humanos para ser cada vez más inteligentes. Antes las personas aprendíamos las tecnologías; cada vez que salía una nueva teníamos que aprender a usarla; ahora la tecnología aprende de las personas y de ella misma –ver gráfico 6-.

Sistemas de Inteligencia Artificial

Permiten a las máquinas "ver, leer, escribir, escuchar, responder…" con tecnologías como el reconocimiento de voz, imágenes y objetos; Procesamiento de Lenguaje Natural (PLN) y otros complejos procesos cognitivos. El vehículo autónomo es un buen ejemplo de Inteligencia Artificial: sin tener ojos ni oídos, el coche autónomo puede ver y oír y realizar esas funciones y muchas más, además de tomar decisiones sin la intervención humana.

Digitalizar la función de riesgos aumenta la capacidad de resiliencia de las compañías

Gráfico 6

Tecnologías y ejemplos de uso en la gestión de riesgos

Tecnología		Qué permite	Caso de uso
	Workflow Automation (iBPM)	Automatización y digitalización de tareas	– Procesos de admisión y seguimiento de riesgos de crédito – Procesos de contratación de productos de activo
	Robotic Process Automation (RPA)	Automatización de procesos y tareas realizadas por personas en la operativa diaria	– Preparación de las tareas y expedientes previos a las tasaciones – Revisión de soportes documentales de los activos registrados
	Data Analytics	Captación y análisis de enormes cantidades de datos	– Análisis de relaciones entre empresas para detectar posible contagio de riesgos financieros – Monitorización en tiempo real y geolocalizada de los eventos de riesgo que se materializan en cualquier parte del mundo
	Machine Learning	Análisis predictivo tras detectar patrones de comportamiento. La máquina aprende de la experiencia	– Predicciones de entradas en mora y prevención y detección del fraude – Prevención y detección del fraude
	Inteligencia Artificial	Reconocimiento de voz, de imágenes, objetos, Procesamiento de Lenguaje Natural, Robótica, etc.	– Onboarding digital (certificación digital del cliente mediante vídeo) – Analítica de textos o voz para detectar sentimiento y posibles indicios de delitos o infracciones – Análisis de texto para prevenir spam y phishing – Monitorización y análisis de conversaciones de traders para segurar el cumplimiento normativo

Fuente: KPMG en España

KPMG

La gestión de riesgos en el mundo digital

Gestión más ágil y efectiva

"La digitalización de la gestión de riesgos deriva en una gestión más ágil y sofisticada, más efectiva y eficiente", subraya Alberto Esteban Henche, socio de *Financial Risk Management* (FRM) de KPMG en España, que argumenta cada uno de los adjetivos calificativos utilizados. Ágil, porque, una vez trazado el camino, "la gestión de riesgos se hace en tiempo real a través de sistemas de visualización de datos de fácil comprensión y con capacidad de respuesta inmediata". Incluso los sistemas pueden sugerir líneas de actuación. Sofisticada, porque "permite afinar al máximo, con un grado de segmentación y granularidad –áreas, negocios, geografías, productos etc. –inimaginable hace unos años". Más efectiva, porque ofrece "visión consolidada con capacidad predictiva, al buscar patrones de comportamiento invisibles al ojo humano que, de alguna manera, actuarán como alerta temprana de riesgos". Más eficiente, porque libera recursos humanos dedicados ahora a tareas manuales y porque un análisis tan afinado y sofisticado, en el sector financiero, permite liberar capital para destinarlo a mayor crecimiento. En todos los sectores permite "aumentar la rentabilidad real del negocio, personalizando el *pricing* al riesgo real asumido".

Los ejemplos de lo que la Inteligencia Artificial puede aportar a la gestión de riesgos son amplios y variados: desde ayudar en el cumplimiento normativo; atención automatizada de los clientes con Procesamiento de Lenguaje Natural y reconocimiento por imagen y voz; monitorización en tiempo real de eventos de riesgos específicos para el negocio en cualquier parte del mundo; análisis de redes de clientes para ofrecer productos o servicios personalizados; detección de valores fuera de rango que puedan llevar a riesgos operativos, análisis de sentimiento de audio o texto y un largo etcétera.

Los clientes son cada vez más conscientes del valor de sus datos y piden a las empresas integridad en su uso

La digitalizacion de la función de gestión de riesgos deriva en una gestión más ágil, porque se hace en tiempo real; sofisticada, porque permite un grado de granularidad inimaginable hace años; efectiva, porque ofrece visión consolidada con capacidad predictiva, y eficiente, porque permite aumentar la rentabilidad real del negocio personalizando el pricing al riesgo real asumido.

Alberto Esteban Henche,
Socio de Consultoría de Riesgos Gestión de Riesgos Financieros (FRM) de KPMG en España

KPMG

La gestión de riesgos en el mundo digital

La clave está en los datos y en la combinación de tecnologías

"Las palancas que soportan la transformación de la función de riesgos son los datos y las nuevas tecnologías, especialmente la Inteligencia Artificial. Aunque ésta se empezó a desarrollar en los años 60, empieza a utilizarse de forma masiva ahora gracias al Big Data, que permite procesar un enorme volumen de datos tanto estructurados como no estructurados –voz, textos, imágenes, vídeos, emails, etc.- antes imposibles de analizar masivamente. La Inteligencia Artificial no es perseguir unicornios. Nuestros clientes nos están solicitando esta tecnología como elemento natural que complementa su transformación digital", dice Eva García San Luis, socia responsable de Data Analytics e Inteligencia Artificial de KPMG en España.

"La combinación de tecnologías es lo que va a permitir un espectacular avance en la gestión de riesgos no solo cuantitativo (más variables y datos), sino también cualitativo (datos no estructurados de gran valor). Y todo ello hace posible obtener *insights* muy valiosos para llevar a cabo análisis predictivos que permitan anticiparse a los riesgos y hacer una gestión más efectiva de los mismos", añade García San Luis.

La integridad de los datos

Las tecnologías disruptivas mejoran la función de gestión de riesgos, pero también introducen riesgos adicionales a vigilar. Uno, evidente, es la ciberseguridad, como veremos en detalle más adelante. Otro, los riesgos tecnológicos derivados de la creciente dependencia de los sistemas tecnológicos –cualquier fallo o interrupción de los mismos puede tener graves consecuencias- y de los riesgos adicionales que puede acarrear la externalización a terceros de los sistemas informático. Cabe mencionar también la creciente importancia del riesgo de modelo por el desarrollo de modelos cada vez más sofisticados, que se nutren de múltiples y diferentes bases de datos a las que luego se aplican complejos algoritmos. Para reducir ese riesgo hay que trabajar con datos de calidad y contar con una política de gobierno del dato adecuada, que garantice un tratamiento correcto y ético de los datos. Pero no solo eso. Como señalaba nuestro informe Guardian of Trust, ¿who is responsible for trusted analytics in the digital age?[3], también las metodologías y el uso que se haga de los datos y las tecnologías debe ser ético para que no se quiebre la confianza entre la empresa y sus clientes, con el resto de stakeholders o con el conjunto de la sociedad.

La integridad de los datos cobra gran importancia en un entorno en el que las empresas pero también los consumidores y la sociedad en general es cada vez más consciente del valor de los datos.

> *La combinación de tecnologías es lo que va a permitir un espectacular avance en la gestión de riesgos no solo cuantitativo (más variables y datos), sino también cualitativo (datos no estructurados de gran valor). Y todo ello hace posible obtener insights muy valiosos para llevar a cabo análisis predictivos que permitan anticiparse a los riesgos y hacer una gestión más efectiva de los mismos.*
>
> **Eva García San Luis,**
> Socia de Consultoría de Riesgos
> Responsable de Análisis de Datos e Inteligencia Artificial
> de KPMG en España

Risk Analytics: los riesgos financieros llevan la delantera

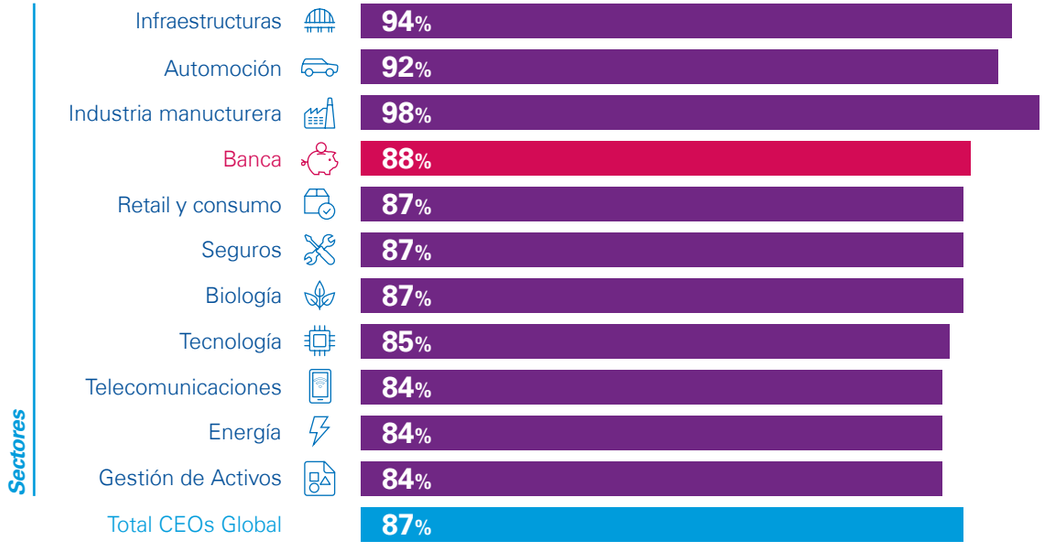
El sector financiero siempre ha ido por delante en gestión y control de riesgos. También ahora.

Después de unos años enfocados al cumplimiento normativo y a las pruebas de *stress test* que los reguladores impusieron a raíz de las carencias detectadas en gestión de riesgos tras la crisis de 2008, las entidades están abordando una profunda digitalización de la función de riesgos. De hecho, figuran entre los sectores más activos en explorar el terreno de la Inteligencia Artificial. Analítica de datos llevan haciendo hace décadas, pero ahora con mucho mayor alcance.

Los bancos lideran la digitalización de la función de riesgos hacia el Risk Analytics

Gráfico 7

Sectores que están explorando la Inteligencia Artificial



Fuente: KPMG Global CEO Outlook 2018. El porcentaje recoge el número de CEOs de cada sector que señaló que ha iniciado la implementación de soluciones de Inteligencia Artificial tanto en algunos procesos de la organización como la puesta en marcha de proyectos piloto limitados.

La gestión de riesgos en el mundo digital

"Los bancos están mostrando un gran interés por las aplicaciones de las tecnologías cognitivas y la analítica de datos en la gestión de riesgos por las ventajas que éstas aportan en la función. Ayuda el empuje de los reguladores, con iniciativas como *Sandbox*, el fenómeno Fintech, con propuestas innovadoras y tecnológicamente muy apalancadas, y el reconocimiento de que, en la era del dato, los bancos tienen un enorme caudal de datos susceptibles de ser analizados para mejorar la experiencia de cliente y la prevención de riesgos. Se están haciendo cosas realmente innovadoras en lo que ya se ha dado en llamar la era del *Risk Analytics* en la banca", apunta Gonzalo Ruiz-Garma, socio responsable del área *Financial Risk Management* (FRM) de KPMG en España.

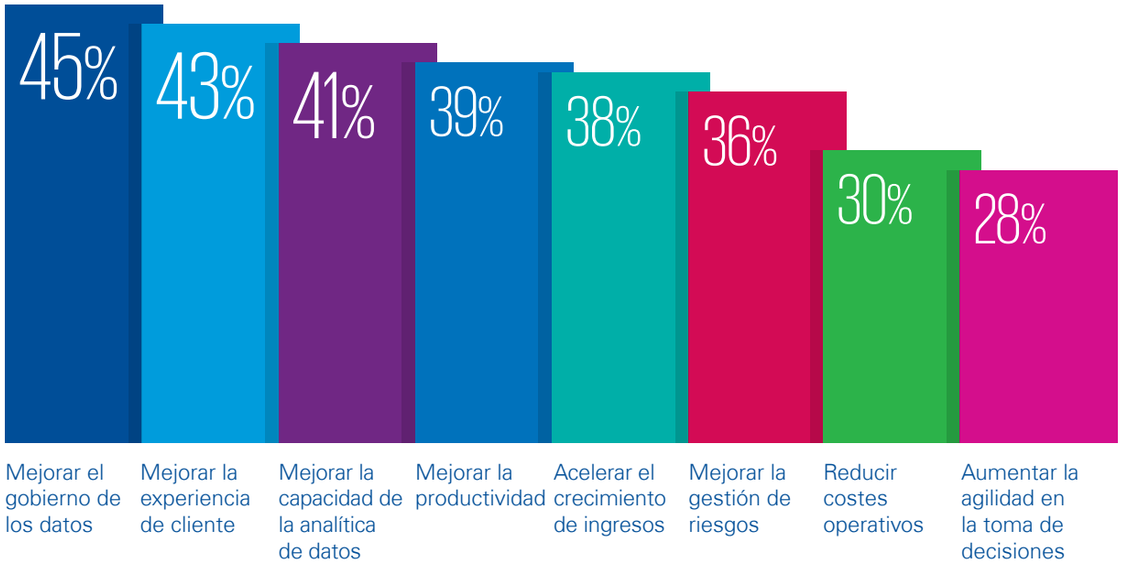
Al pensar en Inteligencia Artificial en la banca, rápidamente nos vienen a la cabeza los *chatbots* que entienden nuestras preguntas, resuelven dudas y hacen sugerencias; el reconocimiento de los clientes por iris, huella dactilar o voz para evitar suplantaciones. Eso es la cara más visible. Internamente se están explorando otros usos de *Machine y Deep Learning* e Inteligencia Artificial, aunque de momento de forma incipiente, según la información recabada a finales de 2017 por el *Financial Stability Board* [4].

Algunos usos son, por ejemplo, la extracción y análisis de texto de documentos para clasificaciones masivas; análisis de conversaciones para evitar fraudes; análisis de redes de clientes para detectar pautas reseñables; análisis predictivos de precios de activos; análisis de sentimiento en redes sociales; analítica base para la concesión de créditos pre-concedidos y crédito rápidos; algoritmos para prevenir y detectar fraudes, y un largo etcétera.

Los bancos utilizan soluciones de Inteligencia Artificial para llevar a cabo grandes innovaciones

Gráfico 8

¿Cuál cree que será el mayor beneficio que le aportará la Inteligencia Artificial en los próximos tres años?



Fuente: KPMG Global CEO Outlook 2018. Recoge las respuestas de los CEOs del sector de banca.

KPMG

La gestión de riesgos en el mundo digital

Los bancos centrales también exploran el potencial de la IA

Además de los bancos privados, muchos supervisores internacionales, que crearon sus propios hubs de innovación, también están explorando el potencial de la Inteligencia Artificial para mejorar la supervisión e incrementar la eficiencia de los procesos de recolección, validación, evaluación y análisis predictivo, según un reciente estudio del *Financial Stability Board* que lleva por título *Artificial Intelligence and Machine Learning in financial services*. Hay muchos e interesantes ejemplos, desde el Banco de Inglaterra, que está validando la calidad de los reportes regulatorios y analizando patrones en la información que le es remitida para detectar y prevenir posibles irregularidades y fraudes, hasta el Banco de Italia que, igual que el de Indonesia, monitoriza las redes sociales para analizar el sentimiento de los depositantes hacia el sistema financiero.

Los supervisores están explotando también las técnicas de Inteligencia Artificial para mejorar la supervisión de entidades y mercados

Gráfico 9

Los supervisores exploran el terreno

Regulador o supervisor	Ejemplo de uso
Bank of England	*Explora Data Analytics* y *Machine Learning* para validar la calidad de los reportes regulatorios y analizar patrones en la información que recibe para detectar y prevenir posibles irregularidades y fraudes.
Autorité des Marchés Financiers du Québec	Ha diseñado un algoritmo capaz de reconocer distintas categorías de campos de texto no estructurados en datos de derivados OTC y ya ha implementado alertas basadas en ese algoritmo para detectar transacciones que no cumplen con los requisitos obligatorios de compensación y liquidación.
Banca d´Italia (BdI)	Presentó un estudio sobre el análisis del sentimiento del texto de los tuits sobre banca para medir la evolución de la confianza de los depositantes en el sistema financiero italiano y detectar a tiempo posibles amenazas a la estabilidad financiera.
Banca d´Italia (BdI)	Para prevenir delitos como el blanqueo de dinero, recoge información detallada de las transferencias y busca correlaciones con noticias aparecidas en la prensa, analizando transferencias y textos.
Singapore Monetary Authority (SMA)	Ha desarrollado un algoritmo para identificar y detectar cuentas sospechosas de las actividades de trading e identificar operaciones que requieren de una investigación más a fondo.
Australian Securities and Investments Commission (ASIC)	Utiliza *machine learning* para identificar campañas engañosas de marketing por parte de asesores financieros no autorizados.
Australian Securities and Investments Commission (ASIC)	Explora *machine learning* para descubrir relaciones poco evidentes entre diferentes sujetos y para detectar en prácticas como blanqueo de dinero o financiación del terrorismo patrones de comportamiento no directamente detectables en las transacciones.
Securities Exchange Commission (SEC)	Utiliza Big Data, analítica de textos y algoritmos de *machine learning* para detectar posibles fraudes y conductas inapropiadas: extrae frases y palabras de las comunicaciones y filings remitidos por los emisores e incluso hace un análisis de indicadores de sentimiento identificando las palabras que tienen connotaciones negativas.

Fuente: Financial Stability Board. Artificial Intelligence and machine learning in financial services.

KPMG

La gestión de riesgos en el mundo digital

Las áreas más proclives a la digitalización

Las áreas o funciones en las que más se está aplicando y/o se ve más potencial para la utilización de *Big Data Analytics, Machine Learning* e Inteligencia Artificial por parte de las entidades financieras son gestión del riesgo de crédito (en todo su ciclo de vida); política de precios; optimización del capital; modelos de *stress test*; análisis de riesgo de mercado; optimización del trading; cumplimiento normativo, detección del fraude y asesoramiento financiero automatizado como son los *roboadvisors*. También se está trabajando ya el emergente riesgo de modelo.

Veamos algunos ejemplos concretos.

Riesgo de crédito: mejoras en todo el ciclo de vida

El Big Data & Analytics está enriquecido los tradicionales modelos de *scoring*, antes basados en solo 10 o 15 variables clave. Ahora se incorporan enormes volúmenes de datos tanto internos como externos. Por ejemplo, para el análisis de préstamos se pueden analizar datos de pagos de recibos, de tarjetas de crédito, débito, transacciones, estadísticas muy segmentadas con históricos y proyecciones sobre datos macroeconómicos o sociales, análisis de sentimiento en los comentarios en redes sociales, etc.

Con estas técnicas, el proceso de originación del crédito es menos costoso, tanto para particulares como para pymes. Para estas últimas, se están utilizando ya ratings crediticios y ubicación geográfica vía geolocalización. Contar con mucha más información es clave para dar entrada en el circuito bancario a personas y pymes que hasta ahora podrían estar excluidas no por falta de calidad de su negocio sino por carencia de rating. Cada vez hay compañías que ofrecen ratings crediticios tanto de pymes como de personas individuales: FICO Score en Estados Unidos y Canadá, Schufa Auskunft en Alemania, Social Credit System en China y otros similares en Japón.

La tecnología ha mejorado la gestión del riesgo de crédito en todo su ciclo, desde originación hasta morosidad y la tasa de recuperaciones

Los bancos están mostrando un gran interés por las aplicaciones de las tecnologías cognitivas y la analítica de datos en la gestión de riesgos por las ventajas que éstas aportan en la función. El sector tiene un enorme caudal de datos susceptibles de ser analizados para mejorar la experiencia de cliente y la prevención de riesgos. Se están haciendo cosas realmente innovadoras en lo que ya se ha dado en llamar la era del Risk Analytics en la banca.

Gonzalo Ruiz- Garma,
Socio de Consultoría de Riesgos
Responsable de Gestión
de Riesgos Financieros (FRM)
de KPMG en España

KPMG

La gestión de riesgos en el mundo digital

Gráfico 10

Oportunidades de mejora en el ciclo de vida del riesgo de crédito

1. Planificación

- Información y alertas sobre clientes o sectores
- Interconexión de clientes (redes neuronales)
- Enriquecimiento de las bases de datos para mejorar la modelización

2. Admisión

- Crecimiento en no clientes
- Inferencia de variables
- Mejora de la estimación de la capacidad de pago

3. Seguimiento

- Ajustes de límites dinámico
- Identificación de necesidades de financiación
- Anticipación de los deterioros de clientes
- Recalibración automática de los modelos
- Modelos predictivos de autoaprendizaje y evolución continua

4. Recuperaciones

- Mejora de las cobranzas
- Estimación de LGD con mayor volumen de datos

El efecto Tech: Fintech, RegTech y SupTech

Primero llegaron las FinTech y las InsurTech. Después las llamadas RegTech: compañías que ofrecen soluciones para llevar a cabo el cumplimiento normativo. Su oferta es abierta a todos los sectores, aunque predominan los servicios específicos para el sector financiero. Y tras las RegTech han llegado también las SupTech, el nombre con el que se conoce a las compañías que ofrecen este tipo de soluciones tecnológicas no a las entidades, sino directamente a los supervisores para ayudarles en su tarea de supervisión del sector financiero. La oferta de las SupTech va desde la estandarización, digitalización y automatización de los procedimientos básicos de supervisión, a herramientas y soluciones que permiten análisis increíblemente granulares y que pueden cambiar radicalmente la supervisión financiera al ampliar enormemente el alcance de la misma.

KPMG

La gestión de riesgos en el mundo digital

Todo esto no solo ha acelerado la rapidez de respuesta de los bancos a las peticiones de crédito -diversos estudios señalan que muchos bancos podrían aprobar hoy en cuestión de segundos el 90% de los créditos a consumidores- sino que supone un gran mejora de la experiencia de cliente para unos usuarios ávidos de respuestas inmediatas.

También ha permitido el desarrollo de nuevos productos, como los seguros de créditos a pymes, los créditos pre-concedidos o los créditos rápidos, que hace años eran impracticables ya que, por su reducido importe y alta recurrencia, o era muy difícil controlar su riesgo o era inviable dar una respuesta inmediata al cliente por el complejo análisis previo de solvencia que se requería.

En el mundo digital, la personalización viene de la mano de la analítica de datos

Políticas de pricing dinámicas y personificadas

"Una de las grandes ventajas del análisis masivo de datos es la granularidad en la segmentación y análisis de clientes. Esto permite llevar a cabo una política de precios mucho más afinada y dinámica y totalmente personalizada. Es curioso que, frente a las relaciones personales del mundo físico, la personalización de la era digital viene de la mano de la analítica avanzada de datos, que es la que permite un análisis, segmentación y oferta de servicios absolutamente personalizado", subraya Gonzalo Ruiz-Garma.

Estos sistemas permiten afinar el análisis del comportamiento de clientes; clasificarlos y reclasificarlos; predefinir sus estrategias; revisar sus precios o alentar la venta cruzada de otro producto con mayor margen; establecer alertas tempranas y tomar medidas al respecto y, por supuesto, medir al detalle la rentabilidad ajustada al riesgo por cliente y productos.

Esto es precisamente están demandando los supervisores: "Si la entidad dispone de herramientas avanzadas como método para mejorar la rentabilidad, podrá desarrollar una adecuada política de fijación de precios, coherente, exhaustiva, que garantice que el precio que se cobra por un producto o servicios se corresponda con su coste total, incluida la prima de riesgos", decía la subgobernadora del BdE en el IX Encuentro Financiero Expansión-KPMG

Anticipar la morosidad al primer síntoma no visible

La tecnología ayuda a detectar los primerísimos síntomas de lo que puede ser una futura entrada en impago o mora, síntomas que a los ojos humanos no son ni evidentes pero que las máquinas pueden encontrar buscando patrones en los data sets y correlaciones con otros datos como la evolución del paro por distritos o barrios, el aumento de los gastos o el cambio en los hábitos de compra –marca blanca frente a producto de marca- de la persona y/o empresa.

También se está aplicando Inteligencia Artificial para mejorar el proceso de recuperaciones. Frente a la multitud de llamadas telefónicas improductivas del pasado a clientes impagados, ahora se analizan las conversaciones para saber cuándo, cómo, quién o por qué canal puede ser más efectivo.

KPMG

La gestión de riesgos en el mundo digital

Simulaciones y modelos de stress test

En la medida en que trabaja con volúmenes masivos de datos, la tecnología permite simular diferentes escenarios y eventos para calcular con precisión el impacto que éstos tendrían en la organización de llegar a materializarse. Esta simulación puede distribuirse y segmentarse tanto como se necesite: por riesgos, negocios, filiales, geografía, productos, etcétera.

Los ejercicios de *stress test* con los que los reguladores prueban la resiliencia de los bancos no se podían llevar a cabo sin este tipo de técnicas. Por ejemplo, el ejercicio CCAR que se exige a los bancos en Estados Unidos requiere considerar el impacto en el negocio de más de 2.000 variables económicas. Además, los modelos van auto-aprendiendo de sus propias experiencias y los *inputs* humanos: cada vez son más inteligentes.

Optimización del capital y de la rentabilidad ajustada al riesgo

La tecnología permite afinar tanto en la gestión del riesgo, bajando a tal nivel de detalle en el cálculo de los activos ponderados al riesgo, que son una herramienta clave para la optimización de los recursos propios, liberando así capital regulatorio para destinarlo a más crecimiento. Y permite hacer una gestión más precisa de la rentabilidad ajustada al riesgo de cualquier línea, negocio, área, producto o incluso cliente.

Automatización de tasaciones

La automatización de procesos permite no solo ahorrar tiempo y dinero, también evitar los errores humanos típicos de las acciones repetitivas. Un ejemplo es la utilización de RPA para automatizar la consulta y verificación de las referencias catastrales en los procesos de tasación. También se puede aplicar para la parametrización y verificación de los expedientes de las carteras de créditos de dudoso cobro, o Inteligencia Artificial para "leer" documentos, seleccionarlos y archivarlos (ejemplo: escrituras, bastanteos, etc.).

Optimización del trading en los mercados de capitales

Hace tiempo que estas tecnologías se utilizan en los modelos de mercado de capitales aunque ahora la sofisticación es mayor por el volumen de datos internos y externos analizados y el aprendizaje cognitivo. El objetivo es optimizar la estrategia y las operaciones de trading, capturar todas las oportunidades que surjan por pequeñas que sean en los precios del mercado; incrementar los márgenes y, en definitiva, aumentar el retorno de las carteras de negociación. Las plataformas de trading automático hace tiempo que están operativas.

Entre las FinTech ha surgido el fenómeno de las SupTech para apoyar con soluciones tecnológicas a los supervisores

KPMG

La gestión de riesgos en el mundo digital

Compliance y reporting

La tecnología es de gran ayuda para la función de compliance, que se ha complicado enormemente en el sector financiero desde los años de crisis: la regulación se triplicó entre 2009 y 2015, un proceso que todavía no ha terminado. De aquí a 2020, los bancos españoles, por ejemplo, tendrán que implantar 100 nuevas regulaciones que ya han sido aprobadas y otras 120 aún en curso, según el informe Claves de la regulación financiera. Impacto y horizonte para las entidades de crédito elaborado por KPMG [5].

El apoyo de la tecnología para verificar con más rapidez y exactitud el cumplimiento normativo es lo que impulsó el sector RegTech. Un ejemplo sería la verificación de los datos de clientes que todas las entidades deben hacer antes de abrir una cuenta; las comprobaciones de clientes que requieren las normativas anti-blanqueo de capitales o la automatización de los procesos que requieren la obligación legal de reportar operaciones sospechosas.

Los sistemas cognitivos ayudan a mejorar la rentabilidad real al afinar al máximo el retorno ajustado al riesgo

Seguros más precisos y personalizados

El sector asegurador es, junto con la banca, uno de los que más ventajas puede obtener del uso de tecnologías disruptivas. Les permite reducir costes, ofrecer mejor experiencia de cliente y evaluar con mucha mayor precisión los riesgos, cuya cobertura es la base del negocio de las aseguradoras.

Cada vez son más las aplicaciones prácticas de estas tecnologías en el sector. Desde la reducción de la siniestralidad mediante la detección temprana de eventos gracias al Internet de la Cosas (IoT) –pensemos en los detectores de fugas de agua y humedad conectados al móvil del usuario–; hasta la personalización de los precios teniendo en cuenta los hábitos del consumidor –el automóvil conectado permite conocer cuándo y cómo se conduce y la información que generan los *wearables* permite afinar y personalizar el precio de las pólizas de salud y de vida–; pasando por la utilización de *chatbots*, que agilizan, personalizan, mejoran y abaratan la atención al cliente. Se trata de avances que tienen que ver con el *front-end* pero, en la medida en que proporcionan información relevante y precisa para mejorar la toma de decisiones y reducir la incertidumbre, tienen una traslación automática en la gestión de riesgos.

Lógicamente, el gran volumen de información (interna y externa, estructurada o no estructurada) que aportan las nuevas tecnologías permite afinar al máximo los perfiles de riesgo y crear nuevos modelos de *scoring* predictivo de clientes basados en *Machine Learning*. Todo ello hace posible que algunas compañías estén reduciendo a minutos la contratación de seguros y la gestión de las reclamaciones por siniestros.

Otra importante aplicación de los algoritmos en el sector asegurador es la detección y reducción del fraude. Ya lo tienen en marcha compañías de diferentes ramos para detectar reclamaciones fraudulentas al comparar automáticamente diferencias sospechosas con miles de siniestros similares. También se están utilizando técnicas de Inteligencia Artificial en la estimación del coste de siniestros para evitar así posibles errores humanos o sesgos. Y, por último, es reseñable apuntar que el sector está utilizando drones para evaluar de forma más precisa los daños de grandes siniestros.

KPMG

La gestión de riesgos en el mundo digital

Algoritmos y riesgo de modelo

La creciente digitalización del sector financiero ha generado nuevos riesgos, sobre los que están llamando la atención los supervisores. Desde 2015, el ciber riesgo es una prioridad supervisora para el BCE, que analiza éste y, en sentido más amplio, el riesgo tecnológico a través de inspecciones in situ.

La sofisticación de los algoritmos tampoco ha pasado desapercibida. "Los algoritmos subyacentes a la Inteligencia Artificial deben diseñarse cuidadosamente y las decisiones incluidas en estos algoritmos tienen que poder entenderse de forma clara tanto por los responsables de los bancos como por nosotros los supervisores. En este sentido, se puede hacer un paralelismo con los modelos internos", decía Ramón Quintana, director general de Mecanismo Único de Supervisión del Banco Central Europeo (BCE) [6].

Cobra así importancia el riesgo de modelo, que en el caso del sector financiero es todavía más relevante.

Los bancos utilizan miles de modelos: para el *pricing* de productos, la detección del fraude, la admisión, seguimiento y recuperación del crédito, el trading y un largo etcétera. Lógicamente, no es lo mismo un fallo en el modelo de blanqueo de capitales que en la valoración de los derivados. El sector debe fortalecer su modelo de gestión de riesgos para gestionar las incertidumbres inherentes a los modelos de Risk Analytics. El riesgo de modelo puede ser potencialmente masivo y es uno de los retos que los departamentos de control y gestión de riesgos deben abordar con mayor precisión en el futuro inmediato [7].

De momento, en el terreno financiero, los supervisores financieros no obligan a cuantificar el riesgo de modelo, pero sí que exigen contar con *framework* que contenga los requisitos señalados por los reguladores con su correspondiente validación aunque hay muchas zonas grises donde cabe la subjetividad [8].

"Hasta hace poco, el riesgo de modelo se veía como un ejercicio más de compliance y no estaba en la agenda del consejo de administración de los bancos. Pero eso está empezando a cambiar y van tomando conocimiento y conciencia de esta importante cuestión. Existen comités específicos de riesgos de modelo e incluso se ha creado una figura específica, el Chief Model Risk Officer (CMRO) que reporta al responsable de riesgos (CRO), y el riesgo de modelo se concibe como una parte integral de la estrategia del banco", subraya Gonzalo Ruiz-Garma, socio responsable d Financial Risk Management (FRM) de KPMG en España.

El riesgo de modelo, junto a la integridad de los datos y el uso correcto de los mismos, es clave para para preservar la confianza de la sociedad. En el caso de los bancos, esto es más relevante todavía. Se puede decir, sin temor a equivocarse, que la necesidad de confianza es algo que no cambiará ni ahora ni nunca en el sector financiero.

Mapa de riesgos: atención a los riesgos no financieros

Geopolítica, digitalización, ciberseguridad, cambio climático, los riesgos que más preocupan a los CEOs.

El mapa de riesgos global muestra una creciente preocupación de los gestores por los riesgos no financieros, esos nuevos riesgos derivados de fenómenos como la globalización, la digitalización, los cambios demográficos y los cambios climáticos y medioambientales.

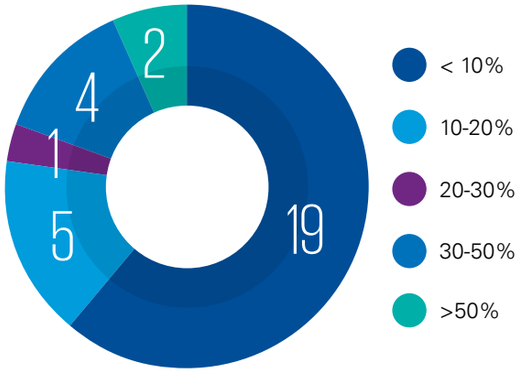
Su impacto es creciente en los resultados y en la imagen de las compañías de cualquier sector, incluido el financiero, según revelaba el informe Navigating bathrough uncertainty [9] elaborado por KPMG que recogía los resultados de una encuesta a los 36 principales bancos europeos. Entre sus conclusiones destacan:

- El porcentaje de pérdidas motivadas por riesgos no financieros se ha incrementado significativamente en los últimos tres años.
- Casi la mitad de las entidades financieras encuestadas sufrieron pérdidas ligadas a riesgos no financieros superiores al 10% de las pérdidas totales. En algunos casos (2 entidades) la proporción de pérdidas superó el 50% -ver gráfico 11-.
- La otra mitad sufrió pérdidas de hasta el 10% atribuibles directamente a riesgos no financieros.
- El 80% augura una creciente importancia de los riesgos no financieros en el futuro próximo.
- Todos los bancos, salvo uno, tiene previsto mejorar sus sistemas y estructuras de gestión de riesgos no financieros.

Gráfico 11

Proporción de pérdidas que generan los riesgos no financieros

Pérdidas atribuibles a riesgos no financieros del total de pérdidas de las entidades financieras en los últimos tres años (*)



(*) Encuesta realizada en 2017 a 36 entidades financieras europeas. Los datos de la tarta reflejan el número de entidades que respondieron esa opción.

Fuente: Informe KPMG "Navigating through uncertainty"

La gestión de riesgos en el mundo digital

La importancia de los riesgos no financieros destaca también en el informe CEO Outlook de KPMG [10], en el que, desde 2015, hemos preguntado a los principales CEOs del mundo por los riesgos que más les inquietaban. En 2018, la pregunta se trasladó a 1.300 CEOs globales, entre ellos 50 españoles.

La principal novedad este año es la fuerte irrupción en el top 5 de los riesgos climáticos y medioambientales, que destacan además en todos los sectores analizados.

También cobran importancia todos los riesgos ligados a nuevas tecnologías disruptivas y emergentes. A medida que la tecnología avanza y surgen nuevas herramientas como *Data Analytics, Machine Learning*, Inteligencia Artificial, *Blockchain*, *Internet of Things* (IoT en sus siglas en inglés), impresión 3D y 4D y las que estén por llegar, crece la preocupación por los riesgos, todavía poco claros en algunos casos, que estas nuevas tecnologías pueden generar.

Los riesgos climáticos han entrado con fuerza en el top5 del mapa de riesgos

Disrupción tecnológica

La innovación tecnológica está cambiando la forma en que vivimos y trabajamos. Hay un reconocimiento claro de que la disrupción tecnológica que genera afecta de múltiples formas a la sociedad, la economía y la empresa. Entre las tecnologías más disruptivas destacan la Inteligencia Artificial, el Internet de las Cosas y el Cloud, que generan cambios de paradigma y permiten acelerar la transformación de los procesos de negocio y ayudan las compañías a adaptar sus productos y servicios a las necesidades de cada cliente (Customer-centricity).

Todas estas tecnologías (y otras que se sumarán en breve) eliminan barreras y limitaciones que durante años han frenado la creatividad de los empresarios. Además, generan oportunidades para desmaterializar procesos y reducir de manera importante los tiempos de producción. También cambian totalmente la visibilidad sobre los KPIs de negocio (ahora en casi tiempo real), permitiendo la toma de decisiones en mucho menos tiempo. Todo esto está acelerando al ritmo a que las compañías crecen y multiplican sus ingresos, pero también y al mismo tiempo, al ritmo a que desaparecen o se vuelven actores indiferenciados en la economía digital. Se aceleran los procesos de éxito y fracaso empresarial.

Todo esto explica que el mapa de riesgos de las compañías incluya cada vez más riesgos tecnológicos (donde destacan, por ejemplo, los temas de la ciberseguridad) y los riesgos del ecosistema tecnológico (relacionados a proveedores y partners tecnológicos) al tiempo que se incrementan los análisis detallados sobre el impacto de nuevas tecnologías, poniendo especial énfasis en evaluar el riesgo de no adoptar o retrasar la implantación de algunas tecnologías (pensando que lo podrán adoptar otros competidores, o incluso que surjan nuevos competidores).

Vivimos en un momento único, de vertiginoso avance tecnológico, en el que las compañías, incluso las más tradicionales, se intentan proteger con la incorporación de talento y expertos en sus consejos, en sus equipos de dirección y en todas las funciones críticas del negocio.

Jorge Santos,
Socio de Consultoría de Riesgos
Responsable de IT Advisory
de KPMG en España

La gestión de riesgos en el mundo digital

Gráfico 12

Top 5 riesgos que más preocupan a los CEOs

Global

2018	2017	2016	2015
1 Vuelta al proteccionismo/ territorialismo (*)	1 Riesgo operacional	1 Riesgo de ciberseguridad	1 Riesgo operacional
2 Riesgo de ciberseguridad	2 Riesgos de tecnologías disruptivas y emergentes	2 Riesgo regulatorio	2 Riesgo regulatorio
3 Riesgos de tecnologías disruptivas y emergentes	3 Riesgo reputacional	3 Riesgos de tecnologías disruptivas y emergentes	3 Riesgo estratégico
4 Riesgo operacional	4 Riesgo estratégico	4 Riesgo estratégico	4 Riesgo de la cadena de suministro
5 Riesgos climáticos y medioambientales	5 Riesgo de ciberseguridad	5 Riesgo geopolítico	5 Riesgo con terceros

España

2018	2017	2016	2015
1 Vuelta al proteccionismo/ territorialismo (*)	1 Riesgo operacional	1 Riesgo de ciberseguridad	1 Riesgo estratégico
2 Riesgos climáticos y medioambientales	2 Riesgo de tipo de interés	2 Riesgo con terceros	2 Riesgo operacional
3 Riesgos de tecnologías disruptivas y emergentes	3 Nuevos hábitos de clientes	3 Riesgo de talento	3 Riesgo de la cadena de suministro
4 Riesgo reputacional	4 Riesgo de ciberseguridad	4 Riesgo regulatorio	4 Riesgos de tecnologías disruptivas y emergentes
5 Riesgo de ciberseguridad	5 Riesgo de fraude	5 Riesgos de tecnologías disruptivas y emergentes	5 Riesgo de talento

(*) Ejemplos: renegociación de USA del NAFTA, Brexit etc.

Fuente: KPMG GLOBAL CEO OUTLOOK

KPMG

La gestión de riesgos en el mundo digital

Los riesgos no financieros son los que más preocupan a los gestores

Es evidente que el uso de las nuevas tecnologías incrementa los riesgos para la ciberseguridad, pero no exclusivamente. Las tecnologías emergentes también generan nuevos desafíos –desde estratégicos a organizacionales, operacionales, de talento y hasta éticos- que hay que empezar a gestionar pese a que muchos no están perfectamente definidos todavía.

Otro riesgo que inquieta cada vez más, especialmente ahora que las redes sociales contribuyen a difundir en segundos cualquier noticia, es el riesgo reputacional. Es de los más difíciles de gestionar por su naturaleza subjetiva –se basa en expectativas y percepciones de terceros- y su total transversalidad. Los CEOs señalaron en nuestro *CEO Outlook 2017* que el riesgo reputacional era uno de los que más impactaría en el crecimiento en los próximos años.

El riesgo reputacional ha cobrado fuerza con las redes sociales

Una mirada a la demografía

Decir que la demografía es relevante para las compañías es una obviedad. Pero entender su impacto no lo es tanto. En primer lugar, requiere revisar su influencia en los mercados en los que las empresas compiten: el de capitales, donde se negocian sus títulos; el de trabajo, en el que son oferentes de empleo y demandantes de talento; y, por último, el de bienes y servicios.

Según Pew Research Centre, prestigioso think tank norteamericano, las principales tendencias demográficas actuales se refieren, entre otros, al envejecimiento de la población; al creciente peso económico de los Millennials; a los movimientos migratorios; o, por último, a la bienvenida participación de la mujer en la vida económica. Cada uno de estos cambios ofrece riesgos y oportunidades para las compañías dependiendo de sus modelos de negocio. Algunos son más evidentes que otros. Por ejemplo, los cambios culturales en gustos y valores sociales tendrán necesariamente consecuencias en el mercado de bienes de consumo. Pero también podrían tener otras menos evidentes en las preferencias de los inversores. En lo que se refiere al mercado laboral, algunas implicaciones del envejecimiento de la población son evidentes. Otras lo son algo menos. En definitiva, entender el riesgo demográfico significa entender su influencia en el comportamiento de inversores, consumidores y empleados y, por lo tanto, en el modelo de negocio.

En el último CEO Outlook de KPMG, los primeros ejecutivos españoles consideran que vivimos un mundo marcado tanto por la velocidad del cambio como por la creciente incertidumbre. Esta circunstancia invita a aplicar una mirada nueva sobre los riesgos, donde lo importante debe ser la capacidad de entender los factores generadores de incertidumbre y, por ende, de riesgo. La demografía debe necesariamente ser uno de ellos. Así parecen entenderlo los CEOs cuando, en el mencionado informe, resaltan la importancia de entender los cambios generacionales.

Ramón Pueyo,
Socio de Consultoría de Riesgos
Responsable de Sostenibilidad y Gobierno Corporativo de KPMG en España

KPMG

La gestión de riesgos en el mundo digital

Volatilidad geopolítica

Aunque la geopolítica no es algo nuevo, en los últimos años han venido ganando protagonismo en las agendas de los altos directivos y de sus consejos de administración como consecuencia de la rapidez y trascendencia con la que se vienen desarrollando los acontecimientos y su impacto sobre las empresas. En efecto, tras varios años de estabilidad y consenso sobre las bondades de la globalización, se han extendido las corrientes proteccionistas y regionalistas, de modo que la mera racionalidad económica ha dejado de ser una restricción para las decisiones políticas.

El Brexit, la situación en Oriente Medio y sus repercusiones en el mercado del petróleo, o las decisiones en materia de acuerdos comerciales internacionales, son sólo algunos ejemplos de la repercusión que la esfera política tiene sobre el entorno económico mundial.

La aparición de estos nuevos riesgos, complejos, interconectados y de rápida propagación, hacen que su gestión se haya convertido en la principal preocupación de los CEOs de todo el mundo, incluidos los españoles, según se refleja en el último informe Global CEO Outlook de KPMG. Por su parte, los consejos de administración han comenzado a requerir que la geopolítica figure en los mapas de riesgos de la empresa, exigiendo los pertinentes planes de contingencia; y también la opinión pública se muestra atenta a las reacciones de los directivos de las grandes corporaciones frente a los acontecimientos políticos.

En este contexto, los CEOs requieren estar constantemente preparados, de modo que, contando con la adecuada información, análisis y estrategia, sepan conocer cómo los riesgos afectan a los modelos financiero, operativo y de negocio de sus empresas.

Surge así la figura del Chief Geopolitical Officer, en la que el CEO asume directamente la gestión de la incertidumbre geopolítica y es capaz de transformar los retos en oportunidades.

Antonio Hernández,
Socio responsable de Internacionalización de KPMG en España.

El riesgo geopolítico cobra importancia en un entorno de creciente volatilidad en la política internacional y efecto contagio por la globalización. La geopolítica, en todas sus derivaciones, debe entenderse como un desafío estratégico más y estar integrada en las evaluaciones periódicas de riesgos.

Otro aspecto muy relevante, que impone grandes desafíos a las organizaciones y requiere por tanto una atención especial para gestionar el crecimiento a largo plazo, son los cambios demográficos que está viviendo la sociedad. Las empresas deben prepararse para atender a los consumidores del futuro, a las nuevas generaciones, que tiene otra forma de ver y entender el mundo y se relacionan con las marcas de una forma distinta.

Cambios demográficos, disrupción tecnológica y riesgos geopolíticos merecen especial atención por parte de las empresas

Ciberseguridad y el efecto cascada

Una brecha de seguridad acaba desatando riesgos adicionales. Contar con sistemas robustos es crítico.

El riesgo de ciberseguridad ha ido evolucionando en los últimos años, desde una posición inicialmente más defensiva a una visión cada vez más proactiva.

"La ciberseguridad ha pasado de ser una cuestión meramente tecnológica a una prioridad estratégica, que debe tutelar y supervisar el consejo de administración, especialmente ahora que los supervisores y reguladores han reforzado su vigilancia. En Europa tenemos el nuevo Reglamento Europeo de Protección de Datos (GDPR en sus siglas en inglés), que exige a las empresas de cualquier país que traten datos de ciudadanos europeos una actitud más proactiva en la gestión de los riesgos de privacidad. Esto incluyendo la realización de análisis de riesgos y definición de su apetito al riesgo, en base al cual se deben establecer las medidas de seguridad, legales y organizativas adecuadas con el objetivo de proteger los datos ante cualquier ciberincidente", explica Marc Martínez, socio responsable de Ciberseguridad de KPMG en España.

Una de cada tres empresas reconoce que ha sufrido un ciberataque en los últimos dos años

Gráfico 13

¿Cuánto de preparada está su organización para hacer frente a un ciberataque?

España

Nota. Cuando la suma no da lugar a 100 se debe al efecto de los decimales y al procentaje, siempre mínimo, que contestó "no sabe".

Fuente: KPMG CEO Outlook España

La gestión de riesgos en el mundo digital

El valor estratégico de la ciberseguridad ha ido creciendo a la par que aumentaban y se sofisticaban los ciberataques, demostrando su enorme y rápida capacidad de contagio, como ocurrió en el verano de 2017 con el conocido ataque de *ramsonware WannaCry*, que afectó a cientos de miles de organizaciones en 150 países diferentes.

Una de cada tres empresas reconoce que ha sufrido un ciberataque en los últimos dos años, según el informe 2018 CIO Survey elaborado por KPMG y Harvey Nash [11], en el que se entrevistó a 3.958 responsables de sistemas de compañías de 84 países del mundo. Según esta encuesta, la mejora de la ciberseguridad es una prioridad estratégica para el 49% de los CIOs consultados: de hecho, es una de las prioridades estratégicas que más ha aumentado su peso este año.

Conectividad y vulnerabilidades

El propio avance de la conectividad de las personas y las cosas a Internet, el rápido crecimiento de *cloud* y *open source* y el uso creciente de los datos que esta conectividad genera abre más potenciales vulnerabilidades. Adicionalmente, la mayoría de las infraestructuras de IT heredadas del pasado no fueron diseñadas para este nuevo entorno y las compañías tienen dificultades para adaptarse, no solo en términos de arquitectura sino también de tácticas, controles internos y políticas.

Los directivos sí que son cada vez más conscientes de que una vulnerabilidad de los sistemas de seguridad acaba activando otros riesgos, como el riesgo de cumplimiento normativo, el riesgo reputacional por el daño ocasionado a la marca o el riesgo operacional.

Pese a ello, según el informe *Global CEO Outlook 2018*, solo el 44% de los CEOs españoles (51% globales) se siente totalmente preparado para hacer frente a un ciberataque. Solo en Estados Unidos (71%) y en Australia (60%) se supera la media global.

GDPR, un impulso a otro enfoque cultural

La aplicación del Reglamento Europeo de Protección de Datos (GDPR en sus siglas en inglés) no solo supondrá un impulso a las prácticas de ciberseguridad. También es un punto de partida para adoptar un nuevo enfoque en la cultura corporativa hacia la protección de datos. "Una cultura en la que la transparencia, los derechos de los ciudadanos y la responsabilidad sea algo automático y natural […], de forma que todo el mundo en la organización valore el derecho de los clientes a su privacidad. Sólo se podrá construir un entorno de confianza si las organizaciones contribuyen, con su transparencia, responsabilidad y principios, a que los clientes sean conscientes de la información personal que éstas tienen de ellos y cómo los usan", como explicamos en el informe de KPMG que lleva por título GDPR: privacy as a way of life [12]. La reputación de la compañía dependerá de cómo se adopte este nuevo enfoque.

Contar con sistemas robustos de ciberseguridad es crítico para preservar la confianza de los stakeholders

La gestión de riesgos en el mundo digital

Y eso pese a que un creciente número de CEOs -49% a nivel global y 32% en España- considera que los ciberataques son inevitables y la pregunta no es sí o no, sino cuándo va a ocurrir. Además, mayoritariamente –el 78% de los CEOs españoles y el 55% de los globales- declara que contar con unos sistemas robustos de ciberseguridad es crítico para generar y preservar la confianza de los *stakeholders* o grupos de interés clave.

El 49% de los CEOs globales (32% de los españoles) cree que los ciberataques son inevitables

En general, los CEOs se sienten más preparados para gestionar un cibertaque en relación a las comunicaciones que deben llevar a cabo con los *stakeholders* – así lo declara el 73% de los directivos globales y el 56% de los españoles – que a la hora de detectar nuevas amenazas o contener el impacto en sus operaciones estratégicas –ver gráfico 15-.

Por sectores, Infraestructuras es el que se considera más preparado ante posibles ciberataques, algo comprensible dado el creciente número de ciberincidentes en las llamadas infraestructuras críticas o sectores estratégicos [13] como reseñaba el informe 2018 *Global Risks Report del World Economic Forum (WEF)* [14].

Una buena gestión de los riesgos de ciberseguridad exige "contar con una visión holística del conjunto, dotarse de las herramientas y procesos necesarios para garantizar la seguridad de los sistemas y procesos y, sobre todo, poder anticiparse a los riesgos. Reforzar y prevenir son la clave para construir una empresa realmente resiliente", subraya Marc Martínez.

Soluciones *Deep Learning*

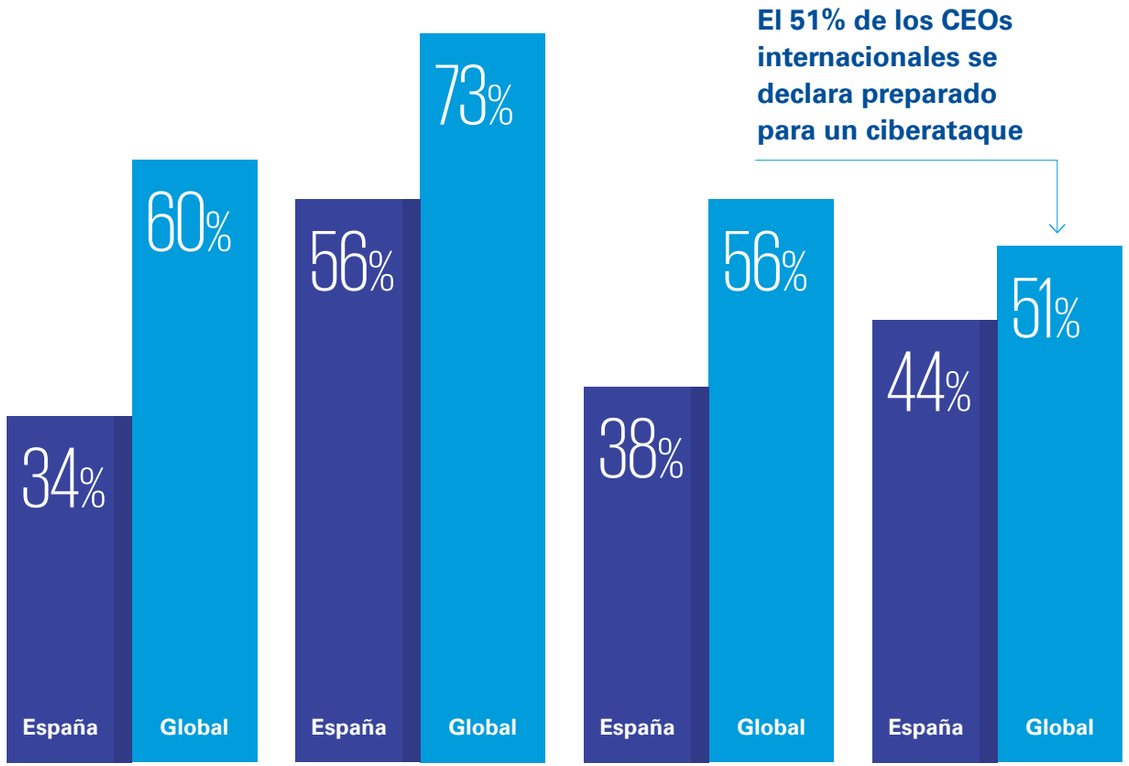
Unas herramientas imprescindibles hoy en día para gestionar el riesgo de ciberseguridad son las nuevas tecnologías como el Big Data Analytics, *Deep Learning* y la Inteligencia Artificial, algo que ya utilizan también los cibercriminales. "Hay que adoptar soluciones de *Deep Learning* para combatir amenazas potentes y convertir así la ciberseguridad en una diferenciador clave para la innovación tecnológica de la empresa", recoge el reciente informe de KPMG *A new era of cyber threats and cyber security* [15].

Estas tecnologías permiten buscar correlaciones entre numerosas fuentes de datos e identificar patrones de comportamiento o anomalías que ayuden a la detección de actividades maliciosas. Algunas compañías lo están utilizando no solo para identificar ciberincidentes, sino para evaluar potenciales vulnerabilidades, construir modelos de identificación de *malware*, intromisiones en la red, detectar ataques de spam o phishing, monitorizar la respuesta y los planes de contingencia y un largo etcétera de soluciones. Este análisis entronca con la labor que llevan a cabo servicios de ciberinteligencia. La combinación de *Data & Analytics* con Inteligencia Artificial es un arma poderosa para ayudar a detectar amenazas antes de que ocurran y reducir el tiempo de respuesta si éstas ya se han materializado.

La gestión de riesgos en el mundo digital

Gráfico 14

¿Cómo de preparada está su organización para un posible ciberataque en relación a los siguientes aspectos?



Capacidad para detectar nuevas amenazas

Capacidad para gestionar la cuestión con stakeholders externos como clientes, reguladores y socios de negocio

Capacidad para contener el impacto de un ciberataque en nuestras operaciones estratégicas

Nivel general de preparación para afrontar un ciberataque

Fuente: KPMG Global CEO Outlook 2018

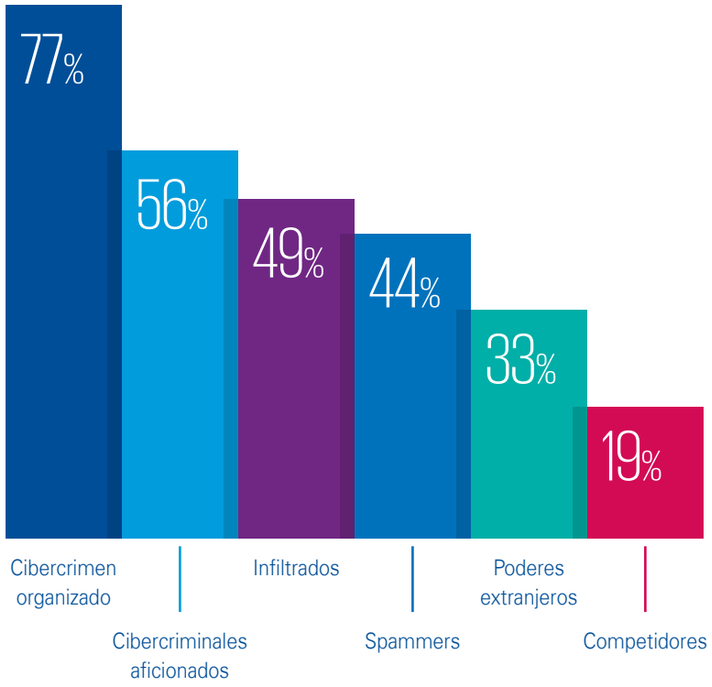
Una buena gestión de los riesgos de ciberseguridad exige contar con una visión holística del conjunto, dotarse las herramientas y procesos necesarios para garantizar la seguridad de los sistemas y procesos y, sobre todo, poder anticiparse a los riesgos. Reforzar y prevenir son la clave para construir una empresa realmente resiliente.

Marc Martínez,
Socio de Consultoría de Riesgos
Responsable de Ciberseguridad de KPMG en España

La gestión de riesgos en el mundo digital

Gráfico 15

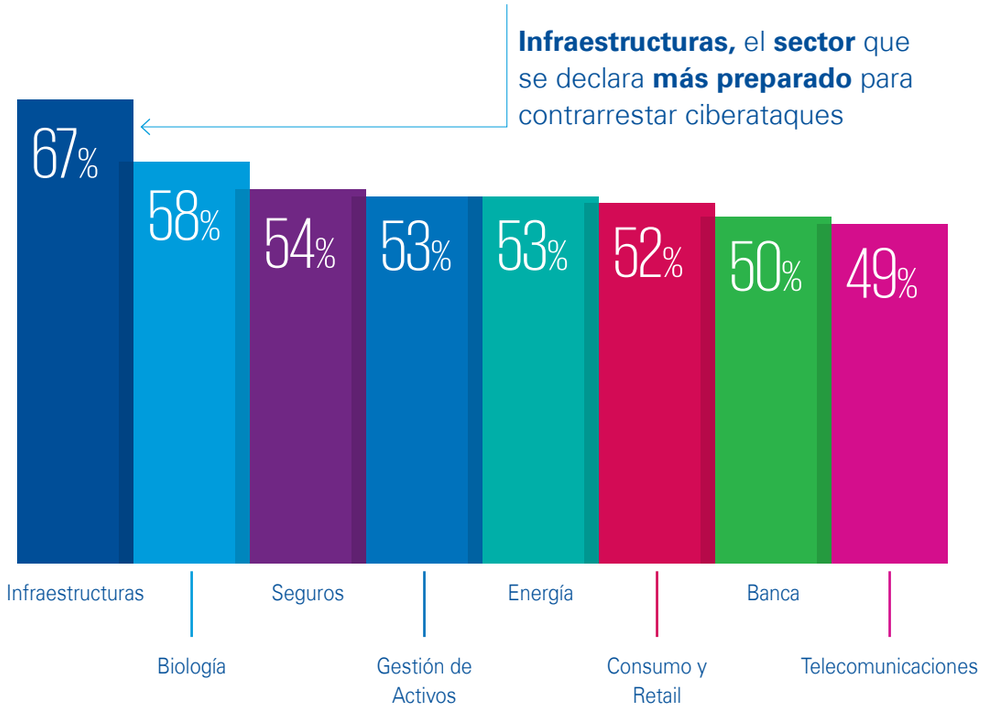
¿Qué tipo de amenaza le preocupa más desde el punto de vista de un ciberataque?



Fuente: 2018 CIO Survey de KPMG y Harvey Nash

Gráfico 16

¿Los CEOs de qué sectores se declaran más preparados para un ciberataque?



Fuente: KPMG Global CEO Outlook 2018

KPMG

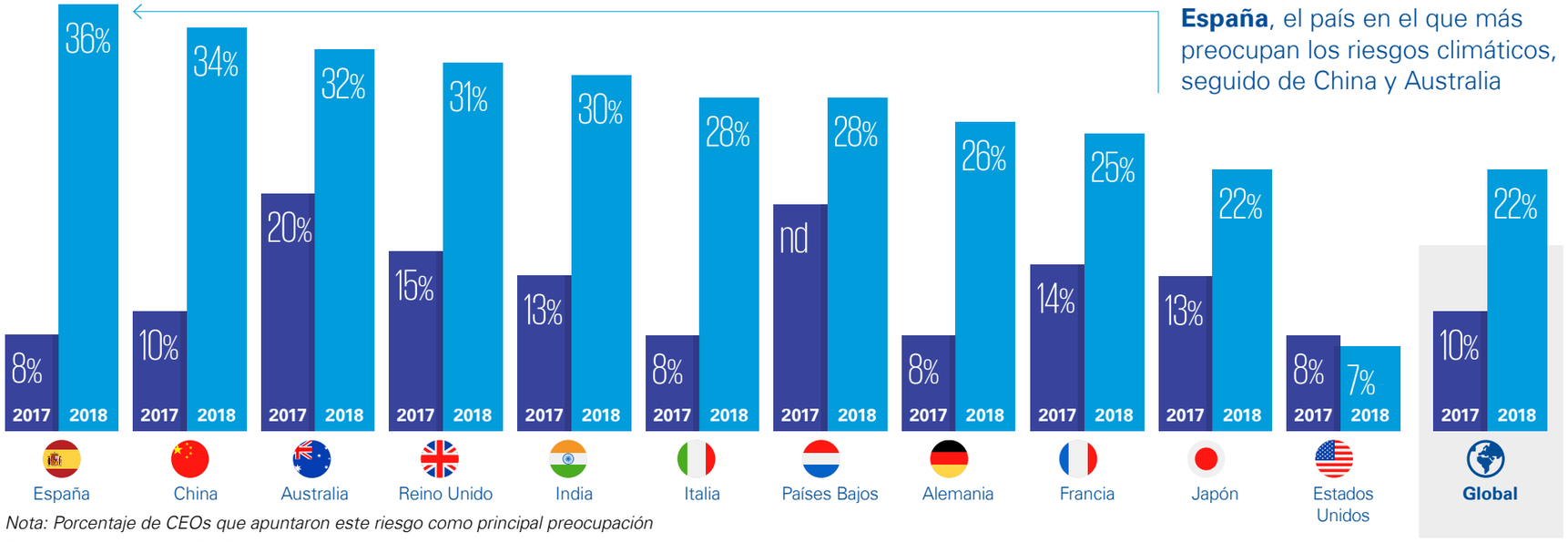
La gestión de riesgos en el mundo digital

Riesgos climáticos y medioambientales, de reconocer a cuantificar

Cada vez más compañías los reconocen y reportan sobre ellos.
Falta poner cifras al impacto.

Gráfico 17

Riesgos climáticos y medioambientales, una preocupación creciente



España, el país en el que más preocupan los riesgos climáticos, seguido de China y Australia

Nota: Porcentaje de CEOs que apuntaron este riesgo como principal preocupación

Fuente: KPMG Global CEO Outlook 2018 y 2017

La gestión de riesgos en el mundo digital

El amplio compromiso para la reducción de emisiones de gases de efecto invernadero logrado de París en 2015 y los episodios atmosféricos extremos han hecho que los riesgos asociados al calentamiento global escalen considerablemente en términos de probabilidad y de impacto en el mapa de riesgos que elabora cada año el World Economic Forum (WEF). De hecho, han alcanzado su punto más alto de los últimos trece años en los que lleva realizándose el informe 2018 Global Risks Report del WEF [16].

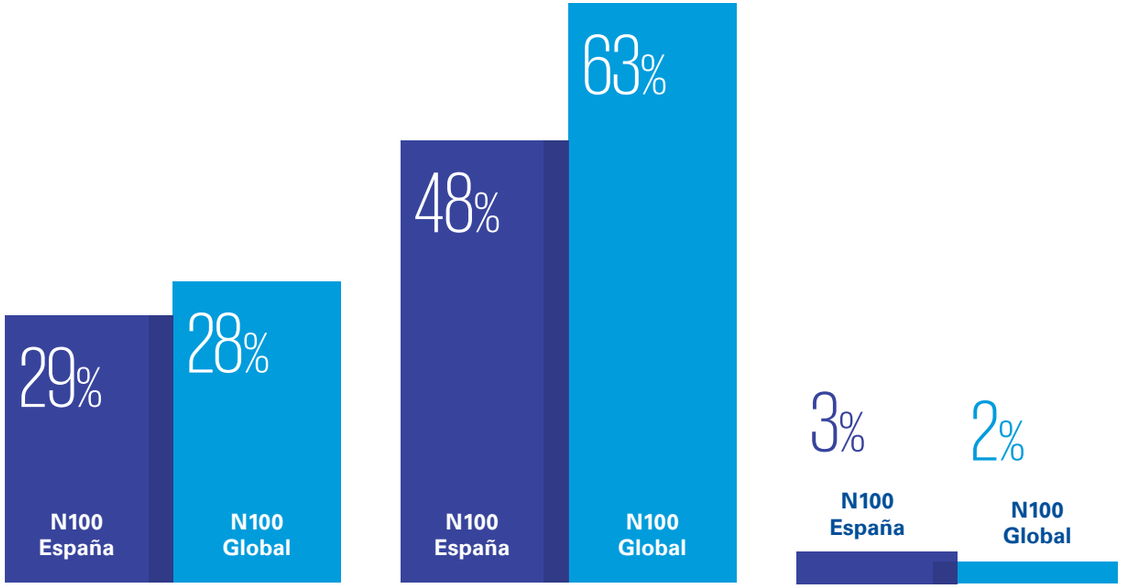
Así lo recoge también nuestro informe 2018 Global CEO Outlook: los riesgos climáticos y medioambientales figuran por primera vez en los cuatro años que lleva haciéndose el informe en el top5 de las preocupaciones de los CEOs. Es la segunda inquietud entre los CEOs españoles y quinta entre los CEOs globales.

Solo una de cada tres compañías reconoce los riesgos financieros que entrañan para su negocio los riesgos climáticos

De los once países analizados en el informe, España es donde los directivos muestran más inquietud por este riesgo. Le siguen China (con alto nivel de contaminación) y Australia (conocida por sus climas extremos). Estados Unidos es donde menos preocupa; es el único país en que este riesgo ha perdido peso entre las inquietudes de los CEOs.

Gráfico 18

Compañías que reconocen, informan y cuantifican los riesgos climáticos



Reconocen que entrañan riesgos financieros para su negocio **(1)**

Además de reconocerlo, aportan una descripción del potencial impacto **(2)**

Además de reconocerlo y describirlo, cuantifican el impacto en términos financieros **(3)**

(1) N100 Global= 4.900 compañías de 41 países del mundo. N100 España= 100 compañías

(2) De las compañías que lo reconocen (1.386 en el mundo y 29 en España), hay un alto porcentaje que adicionalmente los describe (14 en el caso de España)

(3) De las compañías que lo reconocen (1.386 en el mundo y 29 en España), muy pocas lo cuantifican (solo 1 compañía en el caso de España)

Fuente: KPMG 2017 Survey of Corporate Responsability Reporting

La gestión de riesgos en el mundo digital

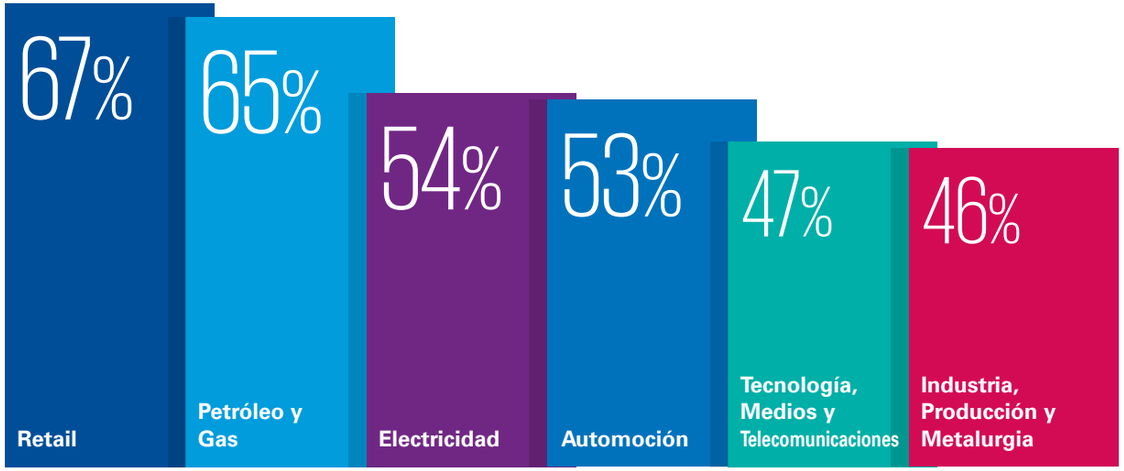
De los 12 sectores analizados en el *2018 Global Ceo Outlook*, el que muestra más inquietud por los riesgos climáticos y medioambientales no es Energía, como podría esperarse, sino Gestión de Activos, lo que refleja la vigilancia creciente de estos riesgos por parte de los inversores. Le sigue el sector de Seguros, que asegura y soporta parte de las pérdidas que entrañan estos riesgos. Industria, Automoción, Infraestructuras y Consumo y Retail son sectores que también se ven cada vez más afectados por los efectos que en su producción o sus ventas tienen las consecuencias derivadas del cambio climático.

Cuestiones de reporting

Las crecientes regulaciones derivadas de los compromisos de reducción y el interés sobre los impactos climáticos en los balances de las compañías por parte de los inversores y aseguradoras están llevando a cada vez más compañías a informar sobre ellos en sus reportes oficiales al mercado. Pero todavía queda camino por recorrer. Según el informe Corporate Responsability Reporting de 2017 [17] elaborado por KPMG, solo un 28% de las 4.900 compañías analizadas en 49 países del mundo reconoce los riesgos financieros que entrañan para su negocio los riesgos climáticos; el 72% restante no.

Gráfico 19

Los sectores que más reconocen el riesgo climático en sus informes financieros



Nota: El dato refleja el porcentaje de empresas de ese sector. Base: G250= las 250 mayores compañías del Fortune 500 a cierre de 2016

Fuente: KPMG 2017 Survey of Corporate Responsability Reporting

Los riesgos climáticos alcanzan su máximo en 13 años en el mapa de riesgos del World Economic Forum

De las que sí hacen mención al riesgo climático (1.386 compañías de las 4.900 analizadas) un 63% describe el impacto; el 33% lo reconoce pero no describe el impacto y solo un 2% (3% en España) cuantifica realmente en números el impacto financiero potencial de los mismos. Y

La gestión de riesgos en el mundo digital

eso pese a que cada vez son más frecuentes noticias como las pérdidas sufridas por las compañías aseguradoras ante una catástrofe o la caída de las ventas en ciertos sectores (alimentación, agricultura, energía, moda, agua...) por condiciones adversas del clima. El análisis de los sectores que más informan y reconocen los riesgos climáticos en sus informes financieros muestra una fotografía más detallada.

"Incluso entre las empresas más importantes del mundo, es todavía escaso el número de aquellas que facilitan a los inversores indicaciones adecuadas sobre el valor en riesgo derivado del cambio climático […] La presión para que las firmas incrementen sus desgloses crece día a día. Algunos inversores ya están exigiendo con firmeza la divulgación de este tipo de información; determinados países están planteándose aprobar reglamentos que obliguen a ello y algunos reguladores financieros han advertido que la ausencia de identificación y gestión del riesgo climático supone un incumplimiento de la obligación fiduciaria del Consejo. Las empresas deberían actuar con rapidez si no quieren presiones adicionales por parte de los mercados de capitales", dice Ramón Pueyo, socio de Consultoría de Riesgos y responsable de Sostenibilidad de KPMG en España.

En línea con los ODS

Los riesgos climáticos y medioambientales son uno más de los múltiples factores que hoy integran el amplio concepto de Responsabilidad Corporativa que los inversores exigen a las compañías y que forman parte de esos valores intangibles que suman o restan valor a su capitalización bursátil.

Los aspectos que deberían abordar esas políticas de Responsabilidad Corporativa entroncan con los 17 Objetivos de Desarrollo Sostenible (ODS en español y SDG en inglés) que adoptó la Organización de Naciones Unidas (ONU) en septiembre de 2015.

Gráfico 20

Objetivos de Desarrollo Sostenible

Fuente: Web de la ONU

La gestión de riesgos en el mundo digital

Cada vez más compañías informan de los ODS en los informes anuales, pero de ellas, solo el 40% de la muestra analizada (las 250 mayores empresas que integraban el índice Fortune 500 al cierre de 2016) informan tanto de los aspectos positivos como negativos y recogen esta referencia en la visión/mensaje de los primeros ejecutivos. En torno al 25% identifica que los ODS son relevantes para su negocio y requiere adoptar acciones. Pero solo un 8% aporta argumentos económicos y casos de negocio para adoptar esas acciones y apenas un 10% se fija objetivos de mejora, según los resultados del estudio recogidos en nuestro reciente informe How to report on the SDGs [18].

Y eso a pesar de que cada vez es más evidente la relación directa entre la responsabilidad corporativa y su valoración en los mercados. Según el informe ESG, risk and return: a board´s eye view, elaborado por KPMG [19] y basado en una encuesta a casi 900 consejeros y directivos de 41 países distintos, el 47% de los consejeros dice que las compañías que se enfocan seriamente en estas cuestiones tienden a tener una mejor trayectoria y posición competitiva que el resto.

No hay KPIs

La mitad de los encuestados señala que lo que mueve a las empresas a enfatizar estos valores es el riesgo reputacional, así como las propias expectativas de clientes, empleados y otros grupos de interés clave. Pese a ello, los directivos reconocen que estas cuestiones todavía son tangenciales y no están integradas en el *core business* de la empresa, es decir, ni en la estrategia, ni en las operaciones ni en la gestión de riesgos. Hasta el punto de que pocas organizaciones miden su mejora con indicadores específicos (KPIs) o integran estas variables en los programas de remuneración o de asignación de capital.

El consejo de administración tiene un papel clave para liderar el avance que deben realizar las compañías en las cuestiones ESG, impulsando su prioridad estratégica, supervisando y clarificando las responsabilidad del comité y del consejo de administración y mejorando tanto la medición como la comunicación interna y externa de los esfuerzos que está haciendo la organización en estas prácticas.

Para hacer una gestión dinámica y más efectiva de todos los riesgos, en KPMG hemos desarrollado una herramienta propia, *Dynamic Risk Assessment (DRA)*, que utiliza sofisticados algoritmos y analítica avanzada de datos para identificar, conectar y visualizar el riesgo en cuatro dimensiones, identificando no solo impacto y probabilidad sino también relaciones entre riesgos y velocidad de contagio entre los mismos.

Algunos inversores ya están exigiendo con firmeza la divulgación de este tipo de información; determinados países están planteándose aprobar reglamentos que obliguen a ello y algunos reguladores financieros han advertido que la ausencia de identificación y gestión del riesgo climático supone un incumplimiento de la obligación fiduciaria del Consejo. Las empresas deberían actuar con rapidez si no quieren presiones adicionales por parte de los mercados de capitales.

Patricia Reverter,
Directora de Consultoría de Riesgos en Sostenibilidad de KPMG en España

La singularidad del riesgo reputacional

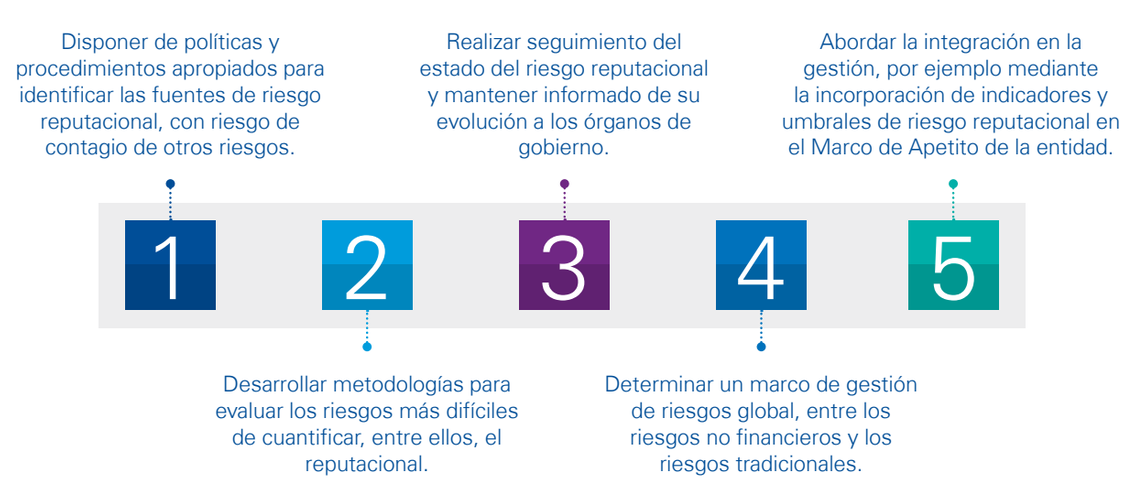
Es un riesgo crítico. Puede ser detonado por mútiples eventos y requiere de una vigilancia constante.

El riesgo reputacional es de los más difíciles de prevenir y gestionar por su naturaleza cambiante y subjetiva. Además, no existen herramientas o metodologías estandarizadas como en el caso de otros riesgos, lo que hace más difícil, aunque no imposible, su cuantificación. Hasta hace unos años –y todavía en muchas empresas- el enfoque tradicional para abordarlo era tratarlo como un caso de gestión de crisis de comunicación y se actuaba más de forma reactiva que proactiva.

La importancia del riesgo reputacional ha crecido durante los años de crisis por la mayor sensibilidad social y también con el desarrollo de las redes sociales, que difunden rápida cualquier acontecimiento –positivo y negativo- protagonizado por una compañía. De hecho, en 2017 y 2018, el riesgo reputacional ha aparecido en el top 5 de riesgos que apuntaban los máximos directivos en el CEO Outlook.

Gráfico 21

¿Qué piden los reguladores financieros sobre el riesgo reputacional?



Fuente: KPMG

La gestión de riesgos en el mundo digital

El riesgo reputacional puede ser detonado por múltiples eventos: brechas de seguridad; fraude; incumplimiento normativo; débiles sistemas de control interno o buen gobierno; falta de transparencia; impactos negativos sociales o medioambientales; rumores o noticias falsas; comportamientos inadecuados de la alta dirección o de los socios de negocio como pueden ser proveedores o aliados de *joint-ventures*... Por eso exige visión multidisciplinar y monitorización constante de lo que piensan de la compañía sus grupos de interés y de lo que se dice sobre ella en cualquier medio, redes sociales, blogs, foros, etc. También hay que contar con procedimientos de debida diligencia externa e interna para monitorizar y mitigar riesgos generados por terceros o por los propios empleados. El riesgo reputacional requiere una gestión y vigilancia constantes, aunque la compañía disfrute en ese momento de la confianza de sus grupos de interés. Y precisamente por eso, para preservarla.

"El futuro tiene la sana costumbre de sorprendernos. Hay muy pocas cosas de las que podamos estar seguros en lo que se refiere al futuro. Me atrevería a decir que una de ellas es que la buena reputación seguirá siendo ingrediente principal del éxito empresarial y que las compañías dedicarán cada vez más atención a preservarla. Las técnicas tradicionales, estáticas, han perdido buena parte de su utilidad en un mundo de creciente dinamismo. Confiar el riesgo a un mapa que revisamos cada seis meses es como conducir mirando a la carretera durante unos instantes cada quince minutos. Ningún problema si la recta es infinita. Pero nunca lo es. El riesgo ha cambiado. También deben hacerlo las técnicas para gestionarlo, incluyendo herramientas que como el análisis de datos, la Inteligencia Artificial o las tecnologías cognitivas ofrecen en términos de la detección, prevención y predicción de riesgos", reflexiona Jerusalem Hernández, directora en Consultoría de Riesgos y Sostenibilidad de KPMG en España.

Los reguladores, en alerta

La creciente importancia del riesgo reputacional ha alertado a los reguladores, especialmente en el sector financiero, sacudido estos años atrás por la crisis financiera y su efecto en la desconfianza hacia el sector. Diferentes normativas financieras tanto europeas – *Supervisory review and evaluation process (SREP)* publicado por la *European Banking Authority (EBA)* en diciembre de 2014 y

El riesgo reputacional es de los más difíciles de gestionar por su naturaleza cambiante y subjetiva

La buena reputación seguirá siendo ingrediente principal del éxito empresarial. Las técnicas tradicionales, estáticas, han perdido buena parte de su utilidad en un mundo de creciente dinamismo. Confiar el riesgo a un mapa que revisamos cada seis meses es como conducir mirando a la carretera durante unos instantes cada quince minutos. Ningún problema si la recta es infinita. Pero nunca lo es. El riesgo ha cambiado. También deben hacerlo las técnicas para gestionarlo.

Jerusalem Hernández,
Directora de Consultoría de Riesgos en Sostenibilidad de KPMG en España

La gestión de riesgos en el mundo digital

actualizadas en 2017– como internacionales –*Proposed enhancements to the Basel II framework* publicado por el Banco Internacional de Pagos (BIS) de Basilea en 2009 – han regulado la necesidad de identificar, evaluar y desarrollar metodologías específicas para supervisar el riesgo reputacional e identificar los eventos y factores internos y externos que pueden ocasionarlo.

No sólo los reguladores y supervisores europeos han sido sensibles a esta cuestión. La CNMV incluye en el "Código de Buen Gobierno de las Sociedades Cotizadas" [20] la evaluación de todo lo relativo a los riesgos no financieros de la empresa, incluyendo los riesgos operativos, tecnológicos, legales, sociales, medioambientales, políticos y reputacionales. Cada día hay más regulaciones y directrices que abordan las pautas y metodologías para una gestión adecuada de este delicado riesgo o que, al menos, lo incorporan como un riesgo adicional que debe estar contemplado en las actividades del día a día de las compañías.

"El riesgo reputacional, junto a otros riesgos como el riesgo de conducta, está ganando cada vez más peso en la supervisión; está en el día a día de las organizaciones y es un aspecto transversal a toda la organización que se tiene en cuenta en la evaluación de SREP de las entidades financieras", señala Mariano Lasarte, socio de Sector Financiero de KPMG.

Puede ser detonado por múltiples eventos, por lo que exige visión multidisciplinar y monitorización constante

El riesgo reputacional resulta más complicado de medir que otros riesgos porque no genera pérdidas directas, como ocurre en riesgos más tradicionales –riesgo de crédito, de fraude, o de mercado-, sino indirectas que pueden traducirse en pérdida de negocio, de clientes, de valor bursátil, de confianza, etc. Sin embargo puede tener un gran impacto. Algunos estudios apuntan que el impacto final en términos de pérdidas de un riesgo reputacional es mucho mayor que las pérdidas directas generadas por el evento que lo disparó. Y según su naturaleza, puede llegar incluso a duplicar esas pérdidas directas iniciales. Aunque tenga un origen presumiblemente pequeño, su dimensión puede crecer en cuestión de segundos o minutos a través de las redes sociales y otros medios digitales.

El riesgo reputacional, junto a otros riesgos como el riesgo de conducta, está ganando cada vez más peso en la supervisión; está en el día a día de las organizaciones y es un aspecto transversal a toda la organización que se tiene en cuenta en la evaluación supervisora de las entidades financieras (SREP).

Mariano Lasarte,
Socio de Sector Financiero
de KPMG en España

KPMG

La gestión de riesgos en el mundo digital

Es clave entender y gestionar la reputación desde el punto de vista de riesgos para poder industrializar su gestión y calibrar su impacto financiero como hacemos con otros riesgos.

Inmaculada González Bayón,
Socia de Consultoría de Riesgos Gestión de Riesgos Financieros (FRM) de KPMG en España

Similitud con el riesgo operacional

Aunque la gestión y el seguimiento del riesgo reputacional presentan un menor nivel de madurez normativo que otros riesgos tradicionales, existe cierto consenso sobre sus similitudes y vinculación con la forma de medir el riesgo operacional. "Es clave entender y gestionar la reputación desde el punto de vista de riesgos para poder industrializar su gestión y calibrar su impacto financiero como hacemos con otros riesgos", señala Inmaculada González Bayón, socia de Financial Risk Management (FRM). Y recalca que "incluso el ejercicio SREP incluye en sus guías la fuerte vinculación entre el riesgo reputacional y el operacional como una pauta a la hora de evaluar el primero, de modo que no se obtenga una evaluación aislada". La similitud estriba en la forma de medirlos, metodología que para el riesgo operacional está fuertemente contrastada.

Gráfico 22

Similitudes y diferencias entre el riesgo reputacional y el operacional

Similitudes

- Alta preocupación por la amplia y diferente distribución de las pérdidas. Requiere modelados más complejos.
- La baja ocurrencia de eventos relevantes de riesgo reputacional lleva a contemplar información externa y sus consecuencias
- Alto grado de contagio entre ambos riesgos y otros.
- Evolución de la cuantificación menos desarrollada. Complejidad para calcular capital por Riesgo Operacional (supresión del Modelo AMA).

Diferencias

- La cuantificación del riesgo reputacional es más compleja por su distribución de pérdidas de baja frecuencia y alto impacto (sin una taxonomía regulatoria clara) y por la ausencia de datos de lo que ha supuesto un evento reputacional, ni siquiera a posteriori.
- No existen bases de datos externas con tanto nivel de detalle de inventario de pérdidas como en Operacional (i.e: ORX).
- No existe tradición de asegurarlo (la reputación corporativa es un concepto más amplio).
- El riesgo operacional debe ser cuantificado aparte del riesgo reputacional.

Fuente: KPMG

La gestión de riesgos en el mundo digital

Aunque la dinámica del riesgo reputacional es diferente a la de otros riesgos y no se ha podido incorporar tiene una metodología estándar porque cada organización tiene sus propias necesidades y diferentes *stakeholders*, las compañías deben revisar su marco de actuación e informes de seguimiento sin perder de vista que el riesgo reputacional puede variar en el tiempo, de la misma forma que varían las percepciones y expectativas de los grupos de interés. Hay prácticas que hoy pueden no presentar problemas y que dentro de unos años generen un impacto muy elevado.

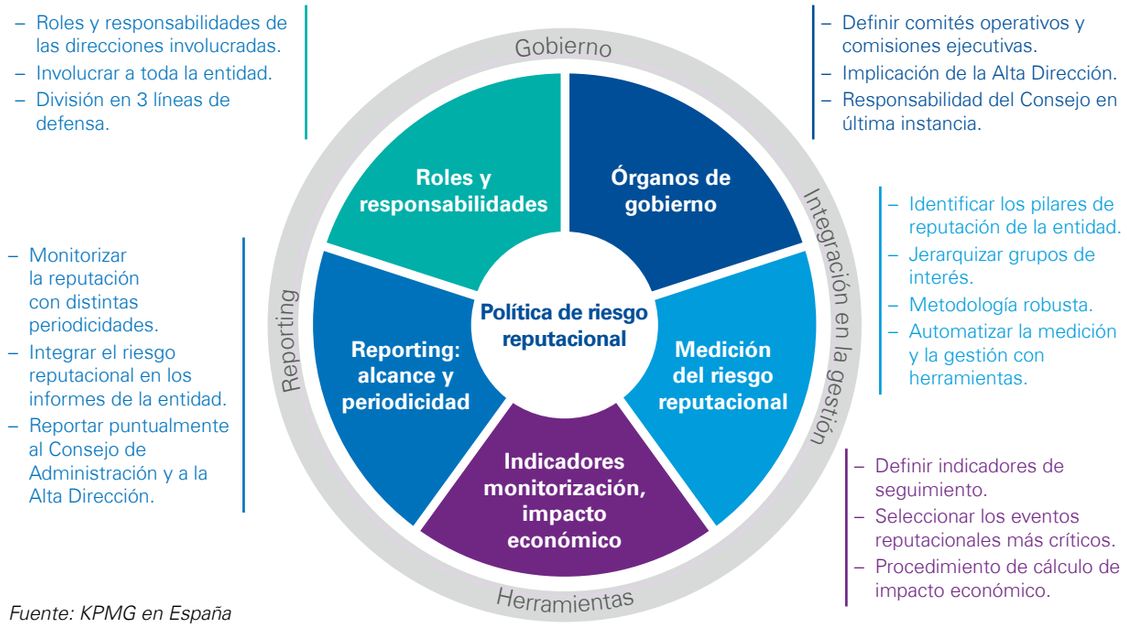
La clave para aplicar una buena gestión es identificar primero y acotar después un mapa de eventos de riesgo reputacional que, además, deben estar jerarquizados por impacto y frecuencia. Para ello, resulta útil incorporar tanto la perspectiva interna –atributos o valores que la organización quiere preservar, conductas previstas, prácticas comerciales, transparencia…- como la externa –percepción de los diferentes *stakeholders*, sensibilidad social... –.

Con una medición periódica –que debe reforzarse con sistemas de monitorización en tiempo real- del desempeño de la compañía y del estado de la confianza y la sensibilidad social, las organizaciones podrán tomar decisiones para actuar sobre el comportamiento corporativo o sobre la relación con los grupos de interés, lo que ayudará a prevenir la probabilidad de que la reputación sufra un daño o reducir su intensidad, en caso de que este daño tenga lugar.

El riesgo reputacional puede variar en el tiempo, de la misma forma que varían las percepciones y expectativas de los grupos de interés

Gráfico 23

¿Qué debe incluir una política de riesgo reputacional?



Fuente: KPMG en España

KPMG

La gestión de riesgos en el mundo digital

Diez claves para una buena gestión del riesgo reputacional

1. Abordar el riesgo reputacional desde las dos perspectivas: riesgos y reputación. Los responsables de riesgo deben validar y promover la metodología.

2. Incluir todas las fuentes en el momento de identificar los eventos de riesgo, entre otros, los mapas de riesgos de la organización o las reclamaciones recibidas por la organización.

3. Evaluar los eventos de riesgo contemplando tanto la perspectiva interna (direcciones involucradas) como la externa (grupos de interés).

4. Priorizar los eventos, clasificados por severidad, para gestionar de manera eficaz los que presenten una mayor amenaza.

5. Cuantificar el impacto económico para facilitar la toma de decisiones de los órganos de gobierno y cumplir con las expectativas de los supervisores.

6. Hacer un seguimiento periódico de la gestión del riesgo reputacional.

7. Supervisar los indicadores de desempeño, la sensibilidad social y la gestión de los grupos de interés para poder anticiparse a la materialización de posibles eventos.

8. Disponer de una política de riesgo reputacional que defina, principalmente, el modelo de gobierno, la integración en la gestión, el reporting y el entorno tecnológico.

9. Automatizar la gestión del riesgo reputacional, permitiendo una visión integrada del modelo, mayor trazabilidad, menor carga de trabajo y menor riesgo operacional.

10. Contar con herramientas de análisis y manuales de gestión de crisis que permitan una respuesta inmediata en caso de que se materialice un evento de riesgo reputacional.

Monitorización en tiempo real

Las herramientas de ciberinteligencia, que monitorizan en tiempo real lo que está sucediendo tanto en la superficie de Internet como en lo más profundo de la web (Deep y Dark Web), es una solución idónea para anticiparse a potenciales riesgos reputacionales, dado que permite analizar en tiempo real qué se dice y se hace sobre la compañía. Puede actuar como alertas tempranas para poner en práctica políticas de remediación. La herramienta de ciberinteligencia desarrollada por KPMG España permite analizar diferentes tipos de perfiles y acciones, personas, grupos, organizaciones, determinar relaciones entre ellos, comentarios, noticias, filtraciones de información, dominios sospechosos, suplantación de identidad, etc. El alcance es mucho mayor que cualquier herramienta de monitorización y vigilancia 24/7 de las redes sociales. Rastrea texto y audio en tiempo real sin límite idiomático, ya que dispone de un traductor automático que analiza los comentarios realizados en más de cien idiomas distintos. Permite crear su propio Data Lake y establecer alertas tempranas personalizadas para detectar a tiempo cualquier posible amenaza.

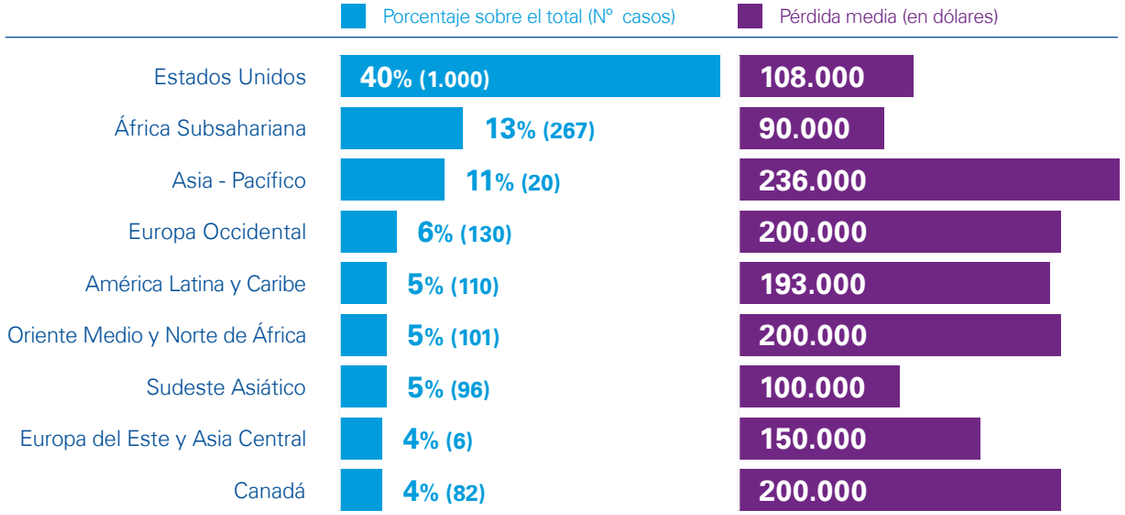
Tecnología para combatir el fraude

Técnicas como la analítica avanzada de datos ayudan a detectar mejor y antes posibles fraudes.

El fraude es uno de los factores que más daño económico y reputacional puede ocasionar a una organización. Puede incluso hasta llevársela por delante, como ocurrió con Enron y WorldCom. Precisamente por eso, por la experiencia del pasado, la lucha contra el fraude ha sido objeto de múltiples recomendaciones de buenas prácticas (ONU, OCDE, etc.) y regulaciones nacionales e internacionales, especialmente en cuestiones de corrupción y prevención del blanqueo de capitales. A nivel internacional destaca la estadounidense *Foreign Corrupt Practices Act* (1977) y la británica UK *Bribery Act* (2010). Recientemente se aprobó también el estándar ISO antisoborno. En España destacan las reformas del Código Penal en 2010 y 2015, que introdujeron la responsabilidad penal de la persona jurídica.

Gráfico 24

Dónde se defrauda más y qué pérdida ocasiona a la empresa



Nota: El estudio analizó un total de 2.960 casos entre enero de 2016 y octubre de 2017

Fuente: Informe Report to the Nations, 2018 Global study on occupational fraud and abuse, de la Association of Certified Fraud Examiners (ACFE)

KPMG

La gestión de riesgos en el mundo digital

A medida que surgían nuevos casos y regulaciones más severas, ha ido creciendo la sensibilidad de la sociedad, especialmente durante estos años de crisis financiera en los que han salido a la luz malas prácticas que se habían ido gestando. Porque el fraude se genera, mayoritariamente, en el interior de las organizaciones. El 65% de los fraudes es cometido por empleados que llevan en la compañía más de seis años; y en un 21% adicional, por ex empleados. En el 62% de los casos hubo colaboración con terceros ajenos a la organización, según los datos recogidos en el informe Global profiles of the fraudster, elaborado por KPMG [21]. Los datos muestran la importancia de que las compañías diseñen procedimientos tanto de debida diligencia interna –para monitorizar los riesgos en la selección de candidatos y la promoción interna - como de debida diligencia externa, destinados a evaluar a los socios de negocio desde una perspectiva de reputación e integridad, que determinen las comprobaciones a realizar antes y durante las relaciones comerciales.

Existe una asimetría clara en cuanto que los defraudadores utilizan mejor la tecnología para cometer fraudes que las empresas para combatirlo

El defraudador tipo

El perfil del defraudador tipo es un hombre de entre 36 y 55 años, lleva trabajando más de seis años en la empresa y tiene un alto cargo directivo o ejecutivo. Más de la mitad de los casos de fraude son reportados por comunicaciones de los propios empleados; un 21% por parte de clientes y un 14% de forma anónima.

Según los datos recogidos en el último informe Report to the Nations [22] de la Asociación de Examinadores de Fraude (ACFE en sus siglas en inglés), los 2.690 casos de fraude analizados durante 2017 generaron unas pérdidas de más 7.000 millones de euros, con una media de 130.000 dólares por caso. El fraude más común sigue siendo la malversación y apropiación indebida de activos (40% de los casos) que, sin embargo, genera bajas pérdidas: 114.000 dólares de media.

Mucho menos frecuentes son los casos de manipulación de estados financieros, como el que llevó a Enron a la quiebra: esta tipología supone sólo el 10% del total pero reportan unas pérdidas medias muy elevadas, nada menos que 800.000 dólares.

Lo que ambos informes ponen de manifiesto es que la debilidad de los controles internos es la causa principal –de más de la mitad- de los fraudes que se cometen y que los avisos y reclamaciones por parte de los propios empleados son la vía más frecuente para su detección. Las líneas éticas están resultando bastante efectivas en este sentido: las organizaciones que cuentan con líneas éticas han reducido un 50% tanto el tiempo de detección del fraude como las pérdidas ligadas al mismo.

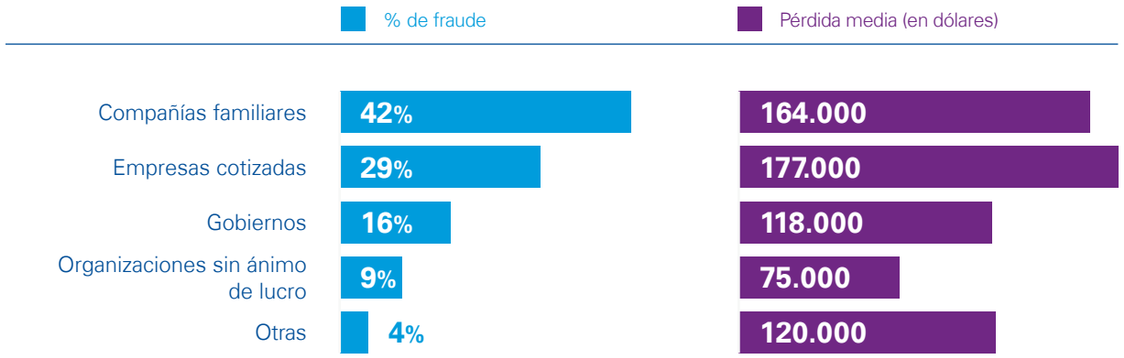
Desde el punto de vista del tamaño, las organizaciones más pequeñas (menos de 100 empleados) suelen tener menos medidas de control y, en consecuencia, sufren una pérdida media por fraude de 200.000 dólares, el doble que las compañías de mayor dimensión (más de 100 empleados). Y desde el punto de vista del tipo de compañías, las empresas familiares se llevan la peor parte: sufren el 42% de los fraudes, con pérdidas medias de 164.000 dólares por caso. La corrupción es el esquema de fraude más extendido en todos los casos y en prácticamente todos los sectores.

KPMG

La gestión de riesgos en el mundo digital

Gráfico 25

El fraude tipo de organizaciones



Nota: El estudio analizó un total de 2.960 casos entre enero de 2016 y octubre de 2017

Fuente: Informe Report to the Nations, 2018 Global study on occupational fraud and abuse, de la Association of Certified Fraud Examiners (ACFE)

Llama la atención el papel creciente aunque todavía asimétrico que juega la tecnología. "Tradicionalmente, la investigación en Forensic se centraba en la contabilidad, en identificar el fraude en los registros contables pero, cada vez con más frecuencia, el fraude tiende a ir más allá para no dejar huellas en la contabilidad. Por eso cada día es más importante utilizar técnicas de inteligencia corporativa y tratamiento masivo de datos que ayuden a detectar la trazabilidad de los activos, analizar correos electrónicos y otro tipo de registros. Nosotros estamos poniendo mucho énfasis en la tecnología para prevenir, identificar e investigar el fraude", explica Fernando Cuñado, socio responsable de Forensic de KPMG en España.

En el 62% de los fraudes hubo colaboración con terceros ajenos a la empresa

eDiscovery Digital Forensics

Hoy prácticamente el 99% de los documentos de cualquier organización son electrónicos y, por tanto, susceptibles de ser fácilmente alterados, ocultados o destruidos. Proteger esa información es crítico, sobre todo en entornos de disputas, negociaciones, arbitrajes o revisiones internas, donde la rápida identificación de la información relevante es crucial para una resolución satisfactoria. Los procesos de eDiscovery optimizan el análisis de grandes cantidades de datos en formato electrónico (obtenidos mediante procedimientos de Análisis Forense Digital), permitiendo identificar y validar la información relevante de cara a su presentación y admisibilidad ante abogados, tribunales o reguladores. Nuestra solución permite acceder a las plataformas en remoto, son de uso intuitivo para la identificación y revisión de documentos, utiliza entornos analíticos de fácil comprensión para hacer el rastreo y recuperación forense de documentos (eliminados, dañados etc.) siguiendo metodologías internacionalmente aceptadas.

La gestión de riesgos en el mundo digital

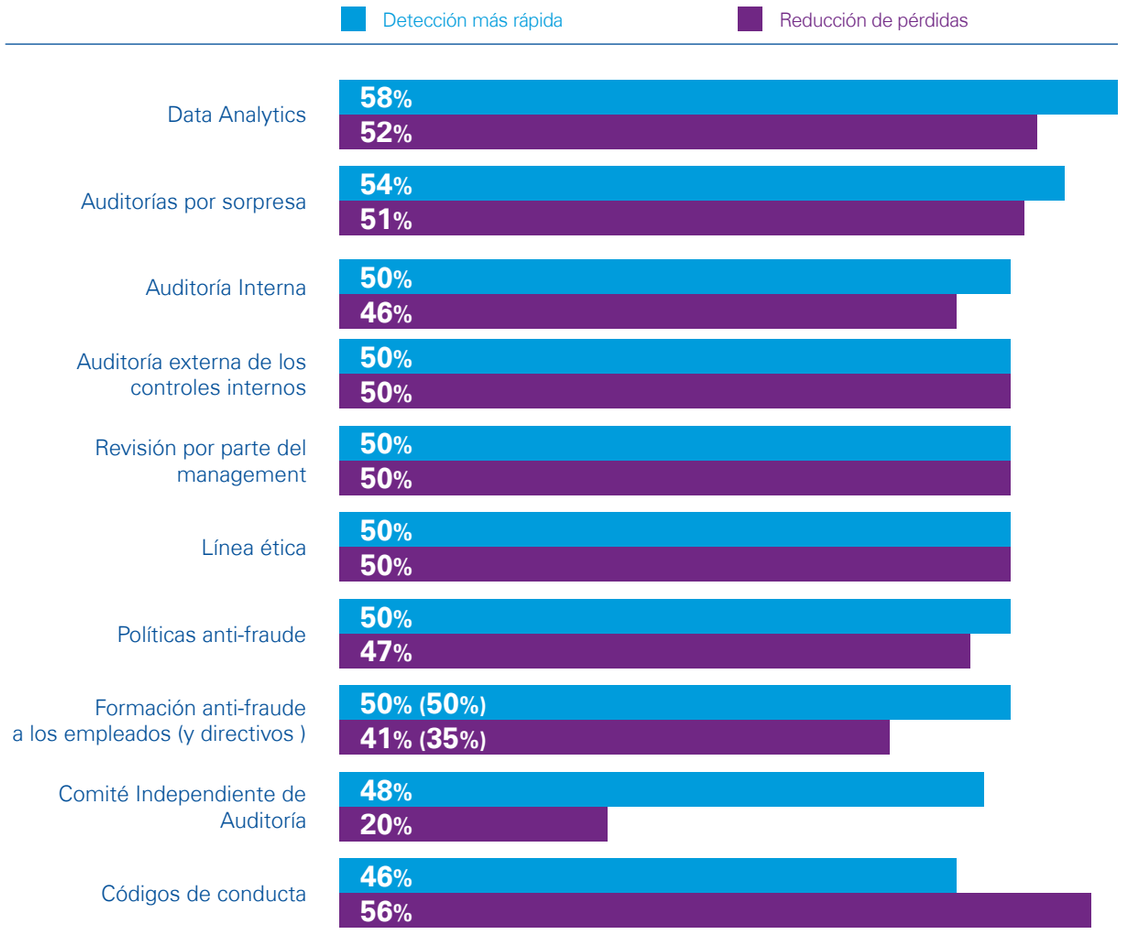
Resulta llamativo que el 24% de los casos de fraude, el uso de la tecnología fue clave para cometer el delito y, sin embargo, sólo un 3% de los casos es descubierto gracias a la tecnología, según el informe de KPMG. La fotografía coincide con lo que apunta el estudio de ACFE: la analítica de datos figura en la cola –en concreto, en el puesto 16 de un total de 18- entre las medidas antifraude más comunes en la empresa. En primer lugar aparecen los códigos de conducta (80% de los casos), seguido de auditorías externas e internas.

Según el citado estudio, solo el 37% de las organizaciones que han sido víctima de fraudes han implementado soluciones de analítica avanzada de datos para prevenirlo. La buena noticia es que las que han implementado estas herramientas han detectado una reducción del 58% en el tiempo de detección del fraude y una disminución del 52% en las pérdidas medias ocasionadas. Las mejoras logradas con la monitorización de los datos superan incluso a las registradas mediante auditorías sorpresa –ver gráfico-.

La analítica avanzada ayuda a detectar las señales de alarma que se repiten en el comportamiento laboral y personal de los potenciales defraudadores

Gráfico 26

Qué impacto tienen algunas prácticas en la detección y reducción del fraude



Nota: El estudio analizó un total de 2.960 casos entre enero de 2016 y octubre de 2017

Fuente: Informe Report to the Nations, 2018 Global study on occupational fraud and abuse, de la Association of Certified Fraud Examiners (ACFE)

La gestión de riesgos en el mundo digital

La contribución de la tecnología a la mitigación y detección del fraude irá aumentando a medida que los datos históricos acumulados por las organizaciones sean mayores e incorporen tantos datos estructurados como no estructurados. La tecnología aplicada a las técnicas de investigación tradicionales como *Forensic Accounting* o *Corporate Intelligence* -identificar conexiones entre personas y entidades-, unidas a las nuevas técnicas de *Data Analytics* (D&A) combinadas con Inteligencia Artificial como *Deep Learning* permiten identificar anomalías o *red flags* que puedan indicar potenciales riesgos de fraude en los libros contables, inventarios, datos de empleados, gastos y cualquier otra información relevante.

La utilización de técnicas de Data & Analytics al fraude reducen a más de la mitad las pérdidas medias potenciales y el tiempo de detección del fraude.

Aplicaciones prácticas de las técnicas de D&A

Corrupción

Las técnicas de análisis permiten identificar pautas de riesgo en delitos de corrupción y cohecho. Se definen algoritmos para identificar posibles indicios de irregularidades.

Blanqueo de capitales

El análisis del tratamiento masivo de datos permite identificar transacciones sospechosas en materia de blanqueo de capitales y clasificarlas para su posterior análisis o reporte. También se pueden crear modelos de evaluación de clientes en base a este riesgo.

Proceso de compras

Analizando la información almacenada por la compañía se pueden identificar patrones irregulares como discrepancias entre pedidos, facturas y albaranes, las condiciones de pagos, pagos duplicados etcétera.

Implantación de alertas

Permiten detectar las posibles irregularidades de manera inmediata e incluso bloquear la transacción sospechosa y evitar que se cometa el fraude.

Manipulación estados financieros

D&A permite hacer un análisis masivo de los asientos contables del libro diario para detectar posibles fraudes, conductas sospechosas o áreas críticas.

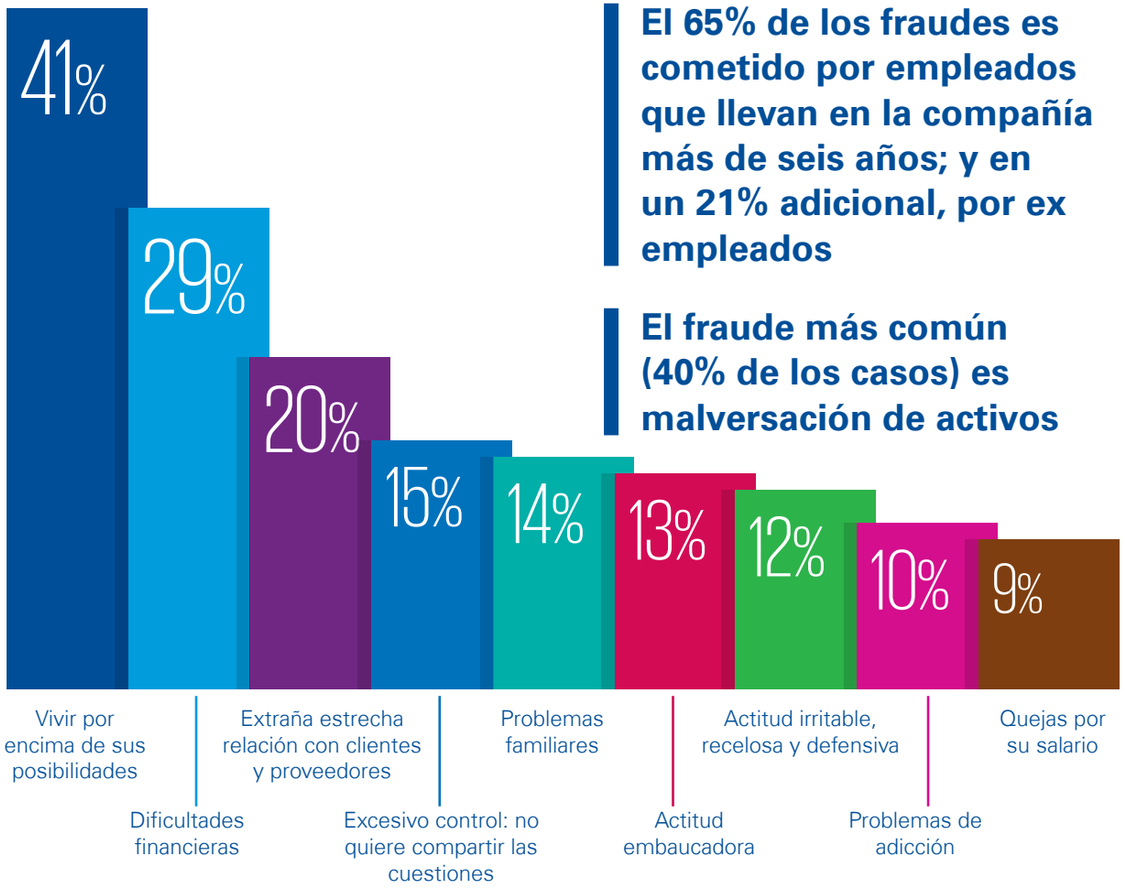
Aplicadas a Recursos Humanos, se podrían analizar las señales de alarma del comportamiento de los potenciales defraudadores. Aunque en el 61% de los casos guardan bien las apariencias –solamente un 9% había sido despedido anteriormente; un 6%, sancionado y un 4%, condenado por conductas fraudulentas- hay un 39% de ocasiones en los que sí que hay señales como un alto nivel de absentismo, pobre desarrollo en sus evaluaciones de mejora, pérdida de empleo, reducción de beneficios o de salarios, etc. También hay otro tipo de comportamientos (recogidos en el gráfico 18) que actúan como señales de alerta temprana: el 85% de los defraudadores muestra al menos una de esas señales de alarma y en el 50% de los casos, aparecen las seis primeras señales, según datos del informe ACFE.

La tecnología permite identificar áreas de riesgo y priorizarlas, analizar los procedimientos, controles y políticas, llevar a cabo una monitorización continua y una vez detectados posibles riesgos, implementar sistemas automatizados que permitan alertar a los responsables de las áreas afectadas.

La gestión de riesgos en el mundo digital

Gráfico 27

Las señales de alarma que muestra el comportamiento del defraudador



El 65% de los fraudes es cometido por empleados que llevan en la compañía más de seis años; y en un 21% adicional, por ex empleados

El fraude más común (40% de los casos) es malversación de activos

Nota: El gráfico muestra la frecuencia en que mostraron esos comportamientos los 2.960 casos analizados. Sólo muestra las diez primeras señales de alarma.

Fuente: Informe Report to the Nations, 2018 Global study on occupational fraud and abuse, de la Association of Certified Fraud Examiners (ACFE)

El fraude tiende a ir más allá y frecuentemente no deja huella en la contabilidad. Por eso cada día es más importante utilizar técnicas de inteligencia corporativa y tratamiento masivo de datos que ayuden a detectar la trazabilidad de los activos, analizar correos electrónicos y otro tipo de registros.

Fernando Cuñado,
Socio de Consultoría de Riesgos
Responsable de Forensic de
KPMG en España y EMA

Conclusiones

1. En un mundo de **cambio constante**, en el que es imposible tener visión sobre el medio y largo plazo pero en el que la **agilidad** de respuesta es clave para sobrevivir, la **gestión de riesgos es una palanca** no solo necesaria sino **crítica en la fijación de la estrategia** de las compañías.

2. No se puede seguir aplicando una **gestión de riesgos analógica** en un **mundo cada día más digital**. Los riesgos son cada vez más dinámicos y devastadores. Las técnicas tradicionales no sirven. Hay que contar con **nuevas tecnologías** que permitan hacer una **gestión de riesgos más sofisticada, predictiva y en tiempo real**.

3. Con la aplicación de múltiples tecnologías como *Big Data Analytics, Machine Learning, Blockchain* o Inteligencia Artificial, sectores como el bancario están liderando la digitalización de la función de riesgos hacia el **Risk Analytics.** Los bancos centrales también están explorando el terreno para mejorar la supervisión. El **sector asegurador** empieza a ver las ventajas de estas **tecnologías disruptivas**.

4. Los **riesgos no financieros** cada vez **ocupan y preocupan más** a las compañías, como muestra el informe CEO Outlook a lo largo de los últimos cuatro años. Desde la **geopolítica** hasta los nuevos **riesgos tecnológicos** pasando por los riesgos que generan los **cambios demográficos** y el cambio climático.

5. Contar con **sistemas robustos de ciberseguridad** es crítico en cualquier compañía para preservar la información y la confianza de los *stakeholders*. Y para ello hay que tomar medidas antes, durante y después.

6. Los **riesgos climáticos y medioambientales** ya forman parte de las agendas estratégicas de las compañías, siendo para muchas de ellas obligatorio reportarlos. En general, las **cuestiones EGS** (acrónimo de *Environmental*, *Social* y *Governance*) ligadas a los Objetivos de Desarrollo Sostenible (ODS) de la ONU están en el punto de mira de inversores, reguladores y organizaciones.

7. El **riesgo reputacional** cada vez preocupa más a las empresas. Es de los más difíciles de gestionar por su **naturaleza cambiante y subjetiva** requiere de una monitorización. Puede ser detonado por múltiples eventos y requiere de una monitorización constante.

8. El **fraude** es un buen ejemplo de cómo la tecnología, frecuentemente utilizada para cometerlo, puede ser también la **solución para prevenirlo**, detectarlo e investigarlo. La analítica avanzada de datos, por ejemplo, permite detectar el fraude y reducir las pérdidas de forma más rápida (Consultar capítulo "Tecnología para combatir el fraude" de este documento).

KPMG

La gestión de riesgos en el mundo digital

Referencias

(1) La aprobación y supervisión de los sistemas de control y gestión de riesgos fue señalada como una de las facultades indelegables del Consejo en el Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital y la reformas posterior recogida en Ley 31/2014, de 3 de diciembre, por la que se modifica la Ley de Sociedades de Capital para la mejora del gobierno corporativo. Ver capítulo III.3.4.3 de las recomendaciones sobre el control y la gestión de riesgos para empresas cotizadas en el Código de Buen Gobierno de la CNMV (febrero de 2015) y la Guía Técnica 3/2017 sobre comisiones de auditoría de entidades de interés público.

(2) Banco de España. Discurso "Modelo de negocio bancario: retos y oportunidades" de Margarita Delgado, subgobernadora del Banco de España, en el IX Encuentro Financiero Expansión-KPMG: "Transformación del sector bancario en el nuevo contexto de innovación digital"

(3) KPMG. Guardian of Trust. Who is responsible for trusted analytics in the digital age?

(4) Financial Stability Board. Artificial intelligence and machine learning in financial services. Market developments and financial stability implications

(5) KPMG. Claves de la regulación financiera. Impacto y horizonte para las entidades de crédito.

(6) Banco Central Europeo. Dicurso de Ramón Quintana, Director General del Mecanismo Único de Supervisión del BCE en el Encuentro Financiero Expansión-KPMG: "Transformación del sector bancario en el nuevo contexto de innovación digital".

(7) KPMG. Informe Managing models in financial services: Transitioning to version 2.0. Recoge los resultados de una encuesta a 35 bancos de Estados Unidos.

(8) Banco Internacional de Pagos de Basilea (BIS) Risk Data Aggregation & Reporting Framework (BCBS239).

(9) KPMG. Report "Navigating through uncertainty"

(10) KPMG. Global CEO OUTLOOK 2018, 2017, 2016 y 2015

(11) KPMG y Harvey Nash. 2018 CIO Survey

(12) KPMG. Informe GDPR: privacy as a way of life.

(13) KPMG Tendencias. Entrevista con Fernando J. Sánchez Gómez, director del Centro Nacional para la Protección de Infraestructuras y Ciberseguridad (CNPIC). El creciente riesgo de los ciberataques a infraestructuras críticas.

(14) World Economic Forum (WEF). 2018 Risks report.

(15) KPMG. Informe A new era of cyber threats and cyber security.

(16) World Economic Forum (WEF). 2018 Risks report.

(17) KPMG. 2017 Survey of Corporate Responsability Reporting

(18) KPMG. Informe How to report on the SDGs.

(19) KPMG. Informe ESG, risk and return: a board´s eye view

(20) CNMV. Código de Buen Gobierno de las sociedades cotizadas.

(21) KPMG. Informe Global profiles of the fraudster

(22) ACFE. Informe Report to the Nations , 2018 Global study on occupational fraud and abuse, de la Asociación de Examinadores de Fraude (ACFE en sus siglas en inglés)

Contactos

Pablo Bernad
Socio responsable de Consultoría de Riesgos KPMG en España
pablobernad@kpmg.es

Gonzalo Ruiz-Garma
Socio de Consultoría de Riesgos Responsable de Gestión de Riesgos Financieros (FRM) KPMG en España
gruiz@kpmg.es

Fernando Cuñado
Socio de Consultoría de Riesgos Responsable de Forensic KPMG en España y EMA
fcunado@kpmg.es

Ramón Pueyo
Socio de Consultoría de Riesgos Responsable de Sostenibilidad y Gobierno Corporativo KPMG en España
rpueyo@kpmg.es

Isidoro Mansilla
Responsable de Auditoría, Control interno y Riesgos KPMG en España
imansillabarreiro@kpmg.es

Jorge Santos
Socio de Consultoría de Riesgos Responsable de IT Advisory KPMG en España
jorgemanuellourenco@kpmg.es

Eva García San Luis
Socia de Consultoría de Riesgos Responsable de Análisis de Datos e Inteligencia Artificial KPMG en España
evagarcia1@kpmg.es

Marc Martínez
Socio de Consultoría de Riesgos Responsable de Ciberseguridad KPMG en España
marcmartinez@kpmg.es