Medición y elaboración de informes de riesgos tecnológicos

Mukul Pareek, CISA, ACA, AICWA, PRM, es especialista en riesgos y trabaja en Nueva York, EE. UU. Cuenta con más de 20 años de experiencia en la prestación de servicios industriales y financieros. Es uno de los editores del Index of Cyber Security, www.CyberSecurityIndex.org, y como tal invita a todos los profesionales del sector a enviar comentarios, información y opiniones sobre la medición cuantitativa del riesgo tecnológico. Toda persona interesada puede enviarle un mensaje a mp@pareek.org.

Hoy resulta difícil pensar en los riesgos operacionales sin relacionarlos con los riesgos tecnológicos. La actual proliferación de aplicaciones basadas en flujos de trabajo, notificaciones activadas por el sistema y bases de datos con "front ends" de páginas web hace que sea imposible distinguir un proceso operacional del sistema en que se ejecuta. Toda falla en el proceso de creación de un evento de pérdida conducirá, casi sin excepción, a la identificación de un control tecnológico que no fue diseñado correctamente o no funcionó. Por ejemplo, cuando en Barings[1] y SocGen[2], entre otras compañías, se produjo una serie de incidentes que tuvieron amplia difusión, se comprobó que uno de los principales factores que causaron esos hechos era el acceso inadecuado a los sistemas.

Esta expansión de los riesgos atribuibles a la tecnología ha afectado considerablemente el trabajo del gestor de riesgos tecnológicos, que ya no solo tiene la responsabilidad de garantizar la seguridad de la información y la protección de los datos, sino que además es "invitado" a participar en innumerables discusiones relacionadas con los procesos de negocios, a fin de analizar los controles de acceso, la segregación de funciones, las jerarquías de aprobación, las notificaciones y el envío automático de comunicaciones a clientes, proveedores y personal con derechos de acceso a información reservada. En consecuencia, el riesgo tecnológico ha cobrado tal relevancia como fuente de riesgo que muchas veces se le destinan departamentos especiales y presupuestos superiores, incluso, al que se invierte en la función central de riesgo operacional.

No obstante, si se le compara con los riesgos crediticios y de mercado, se puede afirmar que las operaciones de cálculo, medición y elaboración de informes de riesgos tecnológicos siguen integrando una disciplina poco desarrollada. Las herramientas de medición de riesgo a las que hoy puede acceder un gestor de riesgos tecnológicos no son más que un conjunto rudimentario de indicadores direccionales de riesgo. La medición y comunicación de riesgos tecnológicos sigue siendo un arte y aún está lejos de convertirse en una disciplina científica. Las herramientas disponibles (matrices de riesgos y controles con distintos niveles de granularidad; paneles con indicadores de color rojo, ámbar y verde; mapas de riesgos; cuadrantes y demás elementos similares para la realización de mediciones no cuantitativas del riesgo) no se aproximan al nivel de sofisticación que poseen las herramientas empleadas por los especialistas en riesgos crediticios y de mercado.

El presente artículo procura identificar opciones más eficaces para la comunicación del riesgo, estableciendo paralelismos con las disciplinas vinculadas a la gestión de riesgos crediticios y de mercado, que han alcanzado un nivel de desarrollo superior. Por consiguiente, el riesgo tecnológico será considerado en este contexto como un importante subgrupo de la categoría general de riesgo operacional. En este artículo, se revisará la eficacia que poseen actualmente los procesos de medición y cuantificación de los riesgos crediticios y de mercado, y se realizará un breve análisis de la aplicación del marco de Basilea en la creación de modelos de riesgo operacional.

COMPARACIÓN DE LOS RIESGOS CREDITICIOS Y DE MERCADO CON LOS RIESGOS TECNOLÓGICOS

Es importante reconocer las diferencias entre el riesgo financiero y el riesgo tecnológico Esto es fundamental, porque estas diferencias básicas son las que impiden que la medición del riesgo tecnológico se realice con la misma objetividad con que se mide el riesgo financiero. A continuación se describen las principales diferencias:

- **Primas por riesgo**: los inversionistas cobran primas a modo de estímulo por la realización de operaciones que conllevan un riesgo crediticio o de mercado. En cambio, la única compensación obtenida por quienes asumen un riesgo tecnológico es el hecho de haber evitado algún inconveniente desconocido (y el costo que supondría el control de ese riesgo). Cuando un gestor de fondos realiza una inversión riesgosa y obtiene un rendimiento superior al índice de referencia, tanto el personal directivo de las empresas como los medios de comunicación pueden comprender fácilmente esta operación. A un gestor de riesgos de TI, en cambio, le costará mucho explicar de manera convincente qué riesgo se ha controlado y qué beneficio se ha obtenido con una inversión de dos millones de dólares en medidas destinadas a preservar la seguridad de la información.
- **Importancia relativa**: en el sector de los servicios financieros, los riesgos crediticios y de mercado son un factor predominante. Estas clases de riesgos pueden motivar el cierre de una institución. Los eventos que suponen un riesgo operacional o un riesgo para los sistemas pueden perjudicar a una empresa, pero es poco probable que se conviertan en causa de cierre, excepto en casos extremos.
- **Disponibilidad de medidas de protección**: la mayoría de los riesgos crediticios y de mercado se pueden compensar mediante la adquisición de posiciones en otros valores. La única medida de protección contra los riesgos tecnológicos, en cambio, es la implementación de controles internos (aunque ahora se puede disponer de un seguro que ofrece cobertura en casos muy puntuales).

¿Le gusta este artículo?

- Lea *IT Control Objectives for Basel II*.

  www.isaca.org/research

- Conozca Risk IT.

  www.isaca.org/riskit

- Acceda al Centro de Conocimiento (Knowledge Center) para obtener más información sobre gestión de y aseguramiento de riesgos.

  www.isaca.org/knowledgecenter

- **Medición**: los riesgos crediticios y de mercado se pueden medir e informar mediante indicaciones de valor en riesgo (VaR, "value at risk")[3], definición de límites y otras herramientas cuantitativas. No obstante, resulta difícil medir el riesgo tecnológico. A la mayoría de los gestores de riesgo les cuesta mucho incorporar nuevas herramientas que vayan más allá que el uso de los indicadores subjetivos de color rojo, ámbar y verde, y sus equivalentes.
- **Fungibilidad**: en los mercados financieros, los activos son idénticos, conllevan el mismo riesgo y requieren las mismas medidas de protección. Por otro lado, a cualquier compañía le resultará difícil proteger un recurso tecnológico en particular (por ejemplo, los routers de la empresa) contra un riesgo determinado, dado que, en general, ningún riesgo puede afectar simultáneamente a todos los activos de esa misma clase, sino solo a una parte. El contraste con los riesgos financieros se puede ilustrar mediante el siguiente ejemplo: cuando se devalúa una moneda, todos los inversionistas que la utilizan se ven afectados, no solo algunos. En el campo del riesgo tecnológico, la materialización de un riesgo se determina de forma binaria, ya que depende de que se produzca o no un evento adverso.

A pesar de las diferencias mencionadas, los riesgos operacionales y tecnológicos tienen muchos elementos en común con los riesgos crediticios y de mercado. En la siguiente sección se analizará la medición y elaboración de informes de riesgos en función de las distintas clases de riesgo (operacional, crediticio y de mercado), con la finalidad de identificar los elementos comunes y las oportunidades de incorporar nuevos conocimientos a la medición y presentación de informes de riesgos tecnológicos.

PARALELISMOS ENTRE LOS RIESGOS DE MERCADO, CREDITICIOS Y OPERACIONALES

Los gestores de riesgos financieros clasifican a los riesgos en tres categorías generales: riesgos de mercado, riesgos crediticios y riesgos operacionales. De los cálculos de riesgo efectuados en el marco de cada una de estas categorías dependen el capital regulatorio y el capital económico, y las empresas toman estos cálculos como referencia para administrar su capital en función de los riesgos que estén dispuestas a asumir y, como corolario, de la calificación crediticia que deseen obtener a partir de la evaluación de las entidades calificadoras de riesgo.

Riesgo de mercado

El riesgo de mercado está vinculado con la posibilidad de que se produzcan pérdidas por las fluctuaciones de los precios del mercado. En esta categoría se incluyen los riesgos de pérdidas por variaciones de precios en instrumentos financieros, tasas de cambio de divisas y materias primas (commodities). Para calcular el riesgo de mercado, es necesario conocer, básicamente, los datos de posición y precios. Con esta información, es posible calcular las correlaciones, la volatilidad y el número del VaR. A primera vista, las diferencias entre el riesgo tecnológico y el riesgo de mercado parecen ser tan grandes que resultaría sumamente difícil establecer cualquier paralelismo.

Una de las principales diferencias entre ambas clases de riesgo está relacionada con los niveles de confianza. Cuando se evalúa el riesgo de mercado, se suele formular una pregunta en términos de intervalos de confianza: ¿cuál es la peor pérdida que se podría producir con un nivel de confianza de, por ejemplo, el 95 por ciento? Para responderla, es necesario calcular la distribución de probabilidad de todos los posibles resultados y observar luego el resultado obtenido en el percentil 5 (límite inferior). Por otro lado, la pregunta que se suele formular al gestor de riesgos tecnológicos tiene que ver con el peor escenario posible. Quizás deberíamos comenzar a evaluar el riesgo tecnológico en función de intervalos de confianza. Es decir, en lugar de centrarnos en el peor resultado posible y dejar que la discusión se desvíe hacia el análisis de escenarios que el personal directivo de la empresa considera improbables, es importante plantear hipótesis plausibles que tengan un determinado nivel de confianza.

Por ejemplo, si se determina que la probabilidad de perder una o varias computadoras portátiles en un año es del 1 por ciento, podríamos afirmar que existe un nivel de confianza del 95 por ciento de que no perderemos ninguna. A un nivel de confianza del 99 por ciento, sin embargo, seguiría existiendo la probabilidad de que se perdiera una o varias computadoras. Si el personal directivo de una compañía quisiera mantener un nivel de confianza del 99 por ciento para reducir ese riesgo, podría tomar la decisión de encriptar las computadoras portátiles para mitigarlo. El nivel de confianza refleja, esencialmente, los riesgos que el personal directivo está dispuesto a correr, es decir su apetito de riesgo.

Riesgo crediticio

El riesgo crediticio es la posibilidad de sufrir pérdidas de activos debido a una reducción en la calificación crediticia o al incumplimiento de pago por parte de los deudores de la compañía. Por lo general, esta clase de riesgos se aplica a préstamos, bonos y exposiciones de contrapartes por posiciones de derivados. Curiosamente, aunque existen numerosos modelos para medir

el riesgo crediticio en el nivel de la cartera, también se están adoptando enfoques de carácter distributivo, en los que se calcula la distribución de las pérdidas esperadas y el riesgo se mide en términos de niveles de confianza en un horizonte temporal determinado (que en general comprende un año). Las pérdidas esperadas son el producto de la exposición al riesgo crediticio (EAD, Exposure At Default), es decir, de la suma que una contraparte adeuda; de las probabilidades de incumplimiento (PD, Probabilities of Default); y de la pérdida en caso de incumplimiento (LGD, Loss Given Default), que da cuenta de las recuperaciones parciales. El cálculo de las pérdidas esperadas se realiza en función de estas tres variables: es decir, la pérdida esperada es igual a EAD × PD × LGD.

En el ámbito de los riesgos tecnológicos, la PD es la probabilidad de que se materialice un riesgo, y la LGD representa la pérdida resultante en caso de producirse el incidente. La exposición al riesgo tecnológico se podría medir empleando un procedimiento un tanto diferente y novedoso:

1. **Exposición**: en el ámbito del riesgo crediticio y de mercado, la exposición se mide en función del tamaño de las posiciones, del tamaño de la cartera o de la suma monetaria de la exposición. El riesgo tecnológico no puede medirse de esta manera, pero no por eso deja de ser mensurable. Los especialistas en riesgo tecnológico suelen ser reacios a realizar todo tipo de suposiciones, dado que, en general, prefieren manejar datos precisos.

   En este sentido sería muy útil un cambio de mentalidad, algo que puede lograrse más fácilmente si examinamos las disciplinas relacionadas con la gestión de riesgos crediticios y de mercado, que han alcanzado un desarrollo superior. La medición de esta clase de riesgos se basa en innumerables supuestos y modelos. Estos supuestos resultan aceptables tanto para el personal directivo de una empresa como para las autoridades reguladoras y los bancos centrales. Por ejemplo, para evaluar los valores de escaso movimiento en el mercado, muchas veces es necesario emplear modelos basados en supuestos. La exposición al riesgo crediticio de un contrato de derivados financieros solo puede determinarse mediante el cálculo de la distribución de los valores que podría adquirir en el futuro, y estas estimaciones se apoyan en una gran cantidad de supuestos. Asimismo, el cálculo de la probabilidad de que un emisor incurra en incumplimiento depende fundamentalmente de la calificación de riesgos y no contempla las características particulares de cada emisor en materia de capacidad financiera. El cálculo de la recuperación en caso de incumplimiento también se basa en supuestos, teniendo en cuenta las incontables variaciones producidas en función del ciclo de negocio y del sector. En otras palabras, las estimaciones y los supuestos pueden ofrecer una base aceptable para la medición de riesgos, siempre y cuando se disponga de un marco conceptual adecuado.

   Si aplicamos la misma analogía al riesgo tecnológico, podríamos arribar a distintas conclusiones respecto de la clase de exposición a la que se enfrentan los gestores de riesgos tecnológicos. Los riesgos tecnológicos pueden clasificarse, a grandes rasgos, en las siguientes categorías:

   - *Filtración de información* que genera pérdidas económicas y perjuicios a la reputación.
   - *Riesgo de continuidad del negocio* por fallas en los sistemas y procesos.
   - *Ataques externos* a la infraestructura, que pueden producir fallas en el funcionamiento de los sistemas o pérdida de datos.
   - *Deficiencias en los procesos y flujos de trabajo* que producen sistemas vulnerables a fraudes, robos o filtración de datos.

   La última categoría es particularmente amplia, ya que abarca innumerables posibilidades. Por citar un ejemplo, podríamos imaginar un sistema con graves deficiencias en su diseño, que no fuera capaz de impedir la pérdida de datos o el fraude informático por carecer de los controles adecuados. Esto incluye elementos como la segregación de funciones en los procesos de negocios y los controles generales de la TI, destinados a evitar esta clase de riesgos.

   El siguiente paso consiste en determinar el grado de exposición de una empresa a cada uno de los factores de riesgo mencionados. En cuanto a los riesgos crediticios y de mercado, las exposiciones se miden en términos monetarios o por el valor de los parámetros (denominados beta) que indican la vulnerabilidad de la cartera a los factores de riesgo subyacentes. El desafío que se plantea a la hora de medir el nivel de exposición a los riesgos tecnológicos radica en la posibilidad de que no exista ningún procedimiento normalizado para realizar la medición y elaborar informes de cada tipo de exposición. No obstante, cubrir este vacío en el nivel de la empresa no debería ser una tarea demasiado compleja. De hecho, podría ser un ejercicio positivo, ya que la empresa tendría la oportunidad de definir las unidades que le resulten más adecuadas para medir la exposición a un riesgo.

   La medición de la exposición podría incluir la cantidad de registros de datos vulnerables, la cantidad de aplicaciones críticas que están expuestas a Internet, la cantidad de cuentas de correo electrónico corporativas y la cantidad de servidores que alojan aplicaciones críticas.

   Por lo tanto, la exposición a los riesgos tecnológicos debería medirse en función de los factores determinantes de esos riesgos, y estar expresada en números o en la unidad que mejor refleje la magnitud de cada riesgo. Al analizar el riesgo crediticio y el riesgo de mercado, el profesional cuenta con una gran ventaja, ya que puede medir todos los niveles de exposición en términos monetarios. Al medir la exposición a los riesgos tecnológicos, en cambio, este procedimiento no siempre resulta conveniente, dado que puede ocultar la verdadera naturaleza del riesgo.

2. **Tasa de error del control (o probabilidad de incumplimiento, cuando se trata de un riesgo crediticio)**: el grado de exposición es, efectivamente, el nivel de riesgo que enfrenta una compañía cuando no se aplica ningún tipo de control. Esta exposición debe compensarse con la aplicación eficaz de controles que estén correctamente diseñados. En el ámbito de los riesgos crediticios, la exposición se compensa con factores atenuantes, como las garantías o prendas. Asimismo, para los especialistas en riesgos tecnológicos, la exposición se compensa mediante la existencia de controles eficientes. Por ejemplo, una empresa puede tener una gran cantidad de servidores conectados directamente a Internet, lo que genera una exposición al riesgo de ataque por ese medio. La presencia de un sistema de detección de intrusiones (IDS) adecuado, así como de otros controles, puede invalidar ese riesgo con gran eficacia, y en ese caso el riesgo residual, o la exposición neta, podría reducirse a cero, si se tienen en cuenta los controles introducidos. La pregunta que surge al examinar este tema está relacionada con la medición de la eficacia de los controles: ¿cómo se puede convertir la eficacia en una tasa de error? Una vez más, las técnicas de auditoría basada en riesgos, que tienen una probada eficacia, y el análisis de muestras ofrecen una respuesta plausible. El análisis de una muestra seleccionada aleatoriamente arrojará una tasa de error esperada para la población total (la precisión del cálculo depende del tamaño de la muestra, y este dependerá, a su vez, del nivel de confianza que se desee obtener en la tasa de error). Si se conoce la tasa de error de un control en particular, se podrá calcular el parámetro real de la población. Por ejemplo, si se estima que el control no logrará impedir ni detectar una determinada falla en el proceso cada 50 transacciones, el parámetro real de la población será del 2 por ciento. Una vez obtenido el grado de exposición y la tasa de error, se puede determinar la frecuencia de falla del control en un período determinado.
3. **Pérdida en caso de fallas en los controles (vinculada a la pérdida en caso de incumplimiento en el contexto de los riesgos crediticios)**: podríamos habernos detenido en el punto anterior. Pero también podemos avanzar un poco más y determinar la pérdida en caso de falla en los controles. Debemos tener en cuenta que no todos los controles generarán alguna pérdida.

El siguiente ejemplo nos permitirá ilustrar lo que hemos analizado en esta sección. Supongamos que una compañía está expuesta a la pérdida de información confidencial a través del sistema de correo electrónico corporativo, y que el sistema de vigilancia de correo electrónico basado en reglas que utiliza la compañía puede bloquear eficazmente el 90 por ciento de los mensajes enviados con esa clase de información. El grado de exposición de la compañía equivale, en este caso, a la cantidad de mensajes de correo electrónico que podrían contener información de carácter reservado y no son bloqueados por el sistema de correo electrónico. Supongamos entonces que, si se vulnerara alguno de los mensajes que no están sujetos al control de la compañía, ésta podría sufrir pérdidas por la suma de US$100,000. Sin embargo, no todos los mensajes que exceden los controles del sistema se envían en forma malintencionada (es posible que la mayoría de esos mensajes no sean vulnerados aunque salgan del perímetro de protección de la empresa), y es probable que la tasa de mensajes enviados en forma malintencionada represente un 0,01 por ciento de los mensajes salientes. En este punto, se puede calcular la pérdida esperada (cantidad bruta de mensajes filtrados × 0.01 por ciento × US$100,000) y la pérdida real en distintos niveles de confianza, para obtener un valor similar al VaR (por ejemplo, utilizando como base la distribución de Poisson, que requiere un solo parámetro: el promedio que acabamos de calcular). Sobre la base de esta información, se puede persuadir al personal directivo de que mejore la eficacia del sistema de vigilancia del correo electrónico (elevando el nivel de "sensibilidad" del sistema lo cual incrementará la cantidad de falsos positivos, algo que demandará tiempo y dinero) hasta alcanzar un nivel en que el personal directivo desee mantener el riesgo residual.

Riesgo operacional

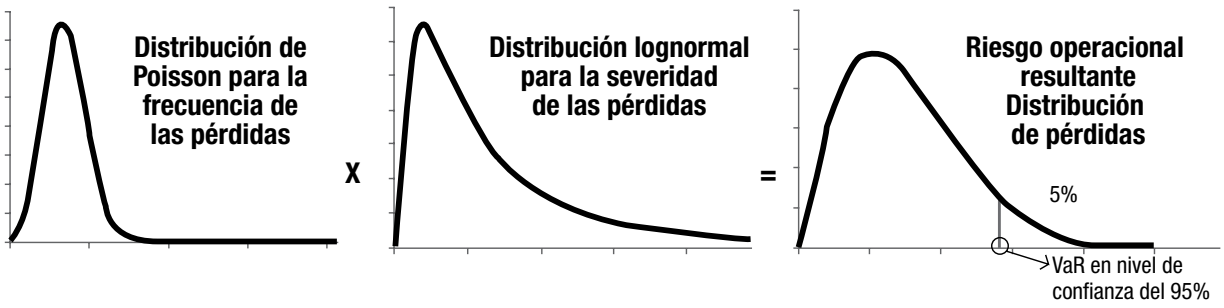
El riesgo operacional es el riesgo de pérdida generado por acción de procesos, personal y sistemas internos inadecuados o inoperantes, o bien por eventos externos. (En el presente artículo, se considera que el riesgo que afecta la reputación de una empresa corresponde a la categoría de riesgos operacionales, aunque el marco de Basilea que se aplica a instituciones financieras lo excluya expresamente.) Como se afirmó anteriormente, el riesgo tecnológico es un componente clave del riesgo operacional.

Una de las críticas que se suele hacer en relación con la gestión de riesgos operacionales es que emplea un enfoque verticalista, al que se considera desconectado de la realidad cotidiana del proceso de gestión de riesgos tecnológicos. Se argumenta que está centrado en el cálculo de números para la adecuación de capital para satisfacer las exigencias de las entidades reguladoras y del personal directivo, y que no ayuda a identificar las medidas que realmente se debería adoptar para abordar un riesgo. Sin embargo, los especialistas en riesgos operacionales utilizan una herramienta fundamental: el análisis de escenarios, que permite calcular la frecuencia y el impacto de las pérdidas y que, al mismo tiempo, logra atraer la atención de los gerentes respecto de la importancia de la gestión de riesgos, mediante la participación en ejercicios de análisis de escenarios.

El marco de Basilea exige la implementación genérica de la técnica de medición avanzada (AMA, advanced measurement approach). Un modelo genérico para un plan de control de riesgo operacional (**figura 1**) funciona de la siguiente manera:

- Los riesgos operacionales se definen como el producto de la frecuencia y severidad de los eventos de pérdida:
  - La frecuencia es la cantidad de eventos de pérdida producidos durante un período dado.
  - La severidad es el impacto que tiene un evento en función de la pérdida materializada.

Figura 1: Planificación de pérdidas por riesgos operacionales



- Frecuencia programada; la frecuencia de las pérdidas se planifica mediante una técnica de distribución adecuada (por lo general, la distribución binomial o de Poisson). Estas distribuciones solo requieren un par de parámetros (incluso es posible emplear uno solo), que se pueden calcular del siguiente modo:
  - Frecuencia de pérdida esperada = Probabilidad de pérdida × Cantidad de eventos, Transacciones, etc.
  - Ejemplo: Supongamos que la probabilidad de fraude con tarjeta de crédito representa el 0.01 por ciento del total de las transacciones realizadas con ese medio de pago, y que la cantidad de transacciones previstas en el horizonte temporal de las pérdidas es 1,000,000. En tal caso, la frecuencia de pérdida esperada, o λ, es igual a 0.01 por ciento × 1,000,000 = 100.
  - Partiendo de algunos supuestos, podemos obtener una distribución de la frecuencia.
- Modelado de la Severidad; la severidad de las pérdidas se mide mediante la técnica de distribución lognormal, y se utilizan sesiones grupales (tipo "focus group"), discusiones de hipótesis, etc., para determinar una media y una varianza (μ y σ).
- El producto de los dos cálculos se obtiene con el método de simulación de Monte Carlo: se toma un valor aleatorio de la distribución de la frecuencia y otro de la distribución de la severidad, se les multiplica y se obtiene un punto de datos. Repita este ejercicio varias veces hasta obtener la cantidad necesaria de puntos de datos para crear una distribución de pérdidas.
- La pérdida se calcula en el percentil quinto o primero, según el nivel de confianza deseado.

CONCLUSIONES PARA LA ELABORACIÓN DE INFORMES DE RIESGOS TECNOLÓGICOS

En el análisis anterior procuramos examinar con atención las herramientas que los gestores de riesgos utilizan en el ámbito financiero, dado que estas herramientas tienen mucho para ofrecer al gestor de riesgos tecnológicos. A continuación mencionaremos las claves que se deben recordar:

1. Piense en términos de niveles de confianza y probabilidades de materialización de un riesgo.
2. No intente comunicar sus conclusiones respecto de los riesgos partiendo del peor de los casos; menciónelo, pero no como única alternativa.
3. Defina el nivel de riesgo admisible ¿Con qué probabilidad estaría dispuesta la compañía o su personal directivo a admitir la materialización de un riesgo determinado? Planifique la implementación de controles que prevean la materialización del riesgo en función de esta probabilidad.
4. Aclare y defina las exposiciones a riesgos y los factores determinantes en términos numéricos.
5. Evalúe los controles supervisando las tasas de error (tanto las que se calculen empíricamente como las que se obtengan mediante análisis de muestras). Realice un seguimiento de estas tasas a través del tiempo.
6. Utilice los análisis de escenarios no solo para descubrir o cuantificar riesgos, sino también como recurso para educar a los gerentes respecto de los posibles riesgos.
7. Realice suposiciones utilizando su propio criterio para cubrir la falta de datos al medir y elaborar informes de riesgos, pero identifique claramente las áreas en las que falta información.
8. Si las suposiciones no coinciden con las observaciones posteriores, corrija los supuestos todas las veces que haga falta.
9. Procure realizar una distribución de pérdidas para determinar las pérdidas por riesgos tecnológicos en distintos niveles de confianza y mejorar los resultados obtenidos con el transcurso del tiempo.
10. Aporte sus propias conclusiones en materia de exposición a riesgos a partir de la observación de las pérdidas producidas en otras compañías del sector.
11. Por último, cuando deba comunicar sus conclusiones sobre los riesgos observados, emplee un vocabulario llano, sin términos especializados; procure alcanzar un nivel de precisión razonable en lugar de aspirar a la precisión absoluta; adopte una visión más amplia; y propicie el diálogo y el intercambio de opiniones.

Si bien es indudable que la medición de riesgos tecnológicos evolucionará con el tiempo, es indispensable que el gestor de riesgos tecnológicos esté atento a las técnicas empleadas para medir el riesgo en otras disciplinas relacionadas y, en la medida de lo posible, que incorpore una o dos herramientas que puedan contribuir para que esta actividad se transforme en una ciencia, sin dejar de ser un arte.

REFERENCIAS

Comité de Basilea para la Supervisión, *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework—Comprehensive Version*

Hull, John C.; *Options, Futures and Other Derivatives*, Prentice Hall, 2005

Index of Cyber Security, *www.CyberSecurityIndex.org*

APOSTILLAS

[1] Banco de Inglaterra, "Report of the Board of Banking Supervision Inquiry Into the Circumstances of the Collapse of Barings", 18 de julio de 1995. El informe identificó diversos factores que condujeron a Barings a la quiebra. Uno de los principales fue que no se segregaron las funciones de Nick Leeson, quien pudo introducir y aprobar transacciones y conciliaciones sin supervisión.

[2] Societe Generale, Resumen de la orden judicial, *www.societegenerale.com/sites/default/files/documents/Summary_of_the_committal_order.pdf*. En enero de 2008, Societe Generale, uno de los dos bancos más importantes de Francia, anunció que Jerome Kerviel, operador de una mesa de valores, había realizado operaciones fraudulentas con dinero del banco, generando pérdidas por una suma de US$7,100 millones. El fraude pudo concretarse sin nadie lo descubriera porque Kerviel no solo era responsable de realizar operaciones comerciales para el banco por el cargo que ocupaba, sino que también tenía responsabilidades incompatibles con esa función, ya que se encargaba de asentar las operaciones en los libros. Para ocultar estos delitos, Kerviel realizaba negocios ficticios, que luego cancelaba e incluso eliminaba de la base de datos electrónica del banco: una clara muestra de las consecuencias que puede tener la asignación inadecuada de derechos de acceso a los sistemas.

[3] El valor en riesgo es un parámetro que se utiliza con mucha frecuencia para medir los riesgos, especialmente los de mercado. En ese contexto, lo que se debe determinar es la distribución futura de los rendimientos o del valor de las carteras. La distribución de los futuros rendimientos o valores no es más que la lista de todos los resultados posibles para una cartera de valores en un horizonte temporal dado (que generalmente comprende dos semanas). El VaR indica, simplemente, la pérdida calculada en el nivel del percentil 5. Es la respuesta a la siguiente pregunta: En un determinado nivel de confianza, y durante un determinado período (y conforme a los supuestos relacionados con las volatilidades, las correlaciones y las distribuciones), ¿qué pérdidas podrían producirse en un horizonte temporal determinado sin exceder el nivel de confianza establecido? Un número de VaR expresado con un nivel de confianza del 99 por ciento indica una probabilidad del 1 por ciento (lo que equivale a dos o tres días al año) de que se exceda este cálculo. El VaR no ofrece una respuesta a la pregunta sobre las pérdidas en el peor de los escenarios, pero permite aplicar un enfoque distributivo a la medición de riesgos en un determinado nivel de probabilidad. Una vez que se conoce la distribución, se sabe todo lo que hay que saber sobre un riesgo; al menos, en teoría. Dado que muchas veces se asume que la distribución es normal, el VaR acaba convirtiéndose en un múltiplo de la desviación estándar.