Naturaleza e impacto de los ciber riesgos

JOSÉ ANDRÉS ACEBO NIÑO

Senior Manager en la actividad FAAS para Seguros de EY en España.

FRANCISCO J. AGUILERA MENÉNDEZ

Técnico en la actividad FAAS para Seguros de EY en España.

GERMÁN SERRANO

Manager de auditoria de Seguros de EY en España.

A mediados de Junio de 2010 se pudo constatar que varias instalaciones nucleares iraníes habían sido atacadas por un virus denominado Stuxnet. Los daños causados por el virus fueron notables y para muchos observadores una de las causas que están detrás del deseo del gobierno iraní de alcanzar un acuerdo sobre la desmilitarización de su programa nuclear. El ataque, supuestamente lanzado por Israel, fue posible debido a una serie de vulnerabilidades iniciales detectadas en los sistemas Microsoft Windows utilizados por Siemmens para el control de determinadas instalaciones industriales. Más allá de las consecuencias geoestratégicas que tuvo el ataque (uno de los episodios más conocidos de guerra cibernética, pero no desde luego el primero), su naturaleza e impacto ponen de manifiesto muchas de las características definitorias de lo que han dado en llamarse ciber riesgos;

a) Cisne negro: Antes de producirse el ataque cibernético, la única preocupación de los estrategas iraníes fue la de prevenirse frente un ataque de tipo convencional, semejante a los que se habían producido previamente (como el bombardeo israelí de las instalaciones nucleares iraquíes de Osirak en 1981). **Su evaluación del riesgo estuvo siempre dominada por la experiencia histórica previa.**

b) Ubicuidad geográfica: El hecho de hallarse las instalaciones iraníes dispersas y más allá del límite operacional efectivo de las fuerzas aéreas israelíes no disminuyó su vulnerabilidad. **La estrategia de diversificación de riesgo tradicional no solo no generó ningún beneficio** sino que muy al contrario, se considera que produjo un aumento del riesgo al ofrecer mayores localizaciones donde poder inocular código malicioso. El riesgo real al que se enfrentaban funcionaba de una forma radicalmente distinta a la que habían conocido hasta ese momento.

c) Interdependencia de los riesgos: El ataque fue posible debido básicamente a una serie de vulnerabilidades de un sistema operativo norteamericano utilizado por un proveedor alemán. Ninguno de estos factores estaban bajo un control directo del gobierno de Irán. Las instalaciones nucleares iraníes estaban por lo tanto a merced de la capacidad (no digamos "interés") de prevenir un ataque de ese tipo por parte de Microsoft y Siemmens. **La interpendencia de los sistemas y proveedores informáticos supone un reto mayúsculo para la eficacia y plena operatividad de las estrategias de mitigación de riesgos.**

d) Dificultad a la hora de identificar a los autores y evaluar el verdadero alcance de los daños: Fueron necesarios varios meses para detectar que se había producido un ataque. Durante todos esos meses el virus continuó activo y produciendo daños, unos daños que aún a día de hoy siguen siendo muy difíciles de evaluar. La impunidad con la que se desarrolló el ataque no solo puso al gobierno de Irán en una situación de indefensión jurídica manifiesta (a diferencia de lo sucedido con acciones armadas anteriores, no hubo ninguna resolución de condena por parte de la ONU respecto de este ataque) sino que limita enormemente el tipo y volumen de represalias posibles frente al agresor. Asistimos a **un escenario en el que el atacante** cuenta con importantes incentivos para llevar a cabo sus acciones debido a que **puede razonablemente esperar salir indemne**. Adicionalmente, **una vez producidos los daños**, los mismos lejos de ser evidentes **son difíciles de identificar y por tanto reparar**.

EL IMPACTO DE LOS RIESGOS CIBERNÉTICOS EN LA ECONOMÍA Y LA SOCIEDAD ACTUALES

Cisnes negros, estrategias de diversificación inadecuadas, interdependencia o riesgo de contagio, y dificultad para evaluar el verdadero alcance de los riesgos, no son, por desgracia, elementos novedosos. Para aquellos familiarizados con las causas y desarrollo de las crisis financieras, las similitudes son evidentes.

¿Pero podría una crisis de confianza global en el entorno cibernético poner a la economía mundial ante el mismo riesgo de colapso ante el que la puso la crisis global de confianza en el sistema bancario de 2007?

Para responder a esa pregunta basta simplemente con analizar la importancia actual y no digamos ya potencial que el entorno cibernético tiene en nuestra economía y

su potencial desarrollo futuro. Un desarrollo futuro que se basa principalmente en la presunción de que existirá en todo momento un entorno cibernético seguro y confiable sobre en el que basar nuestro crecimiento.

Por tanto, el escenario en el que una serie de fallos en cadena conducen a una quiebra global de la operatividad del entorno cibernético, el denominado "Cibergeddon" es indudable que produce enorme inquietud. Tanto instituciones públicas como privadas se encuentran concernidas por el potencial impacto de un suceso como éste. Entre ellas, obviamente, el gobierno de España quien ha incluido la ciberseguridad como uno de los ejes principales en los que debe articularse nuestra seguridad nacional:

"La ciberseguridad no es un mero aspecto técnico de la seguridad, sino un eje fundamental de nuestra sociedad y sistema económico" (Estrategia española de seguridad nacional, 2011).

EL MODELO DE CUANTIFICACIÓN DE CIBER RIESGOS PROPUESTO POR EL FORO ECONÓMICO MUNDIAL EN ENERO DE 2015

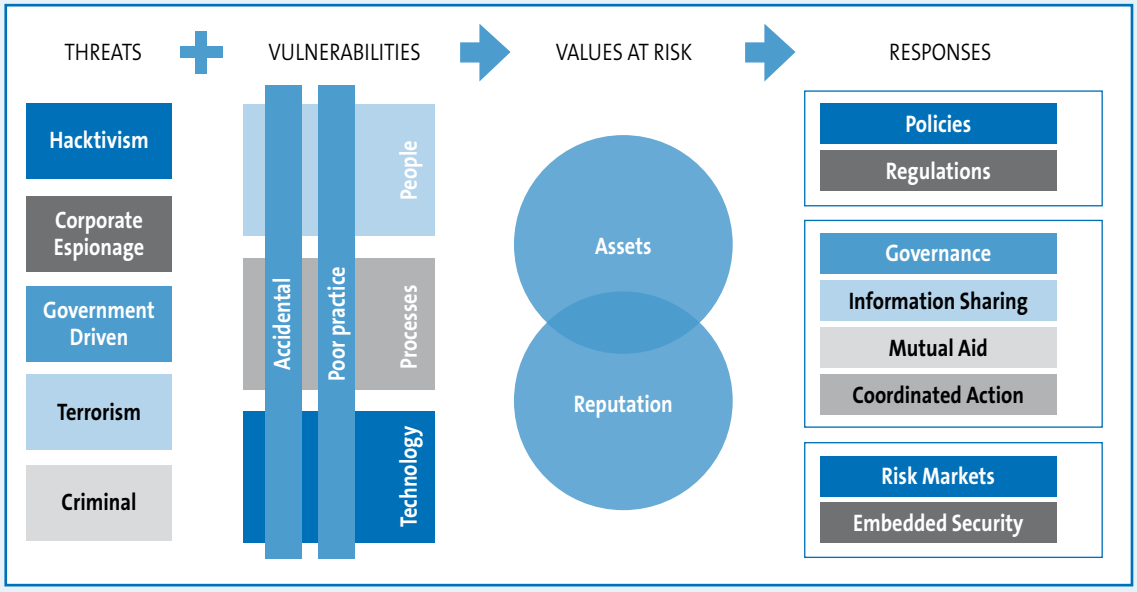
Pero la importancia de estos asuntos trasciende claramente las fronteras de los estados nacionales, es por ello que diversos organismos internacionales han abordado esta problemática desde diversas perspectivas. Entre ellos, cabe destacar el papel jugado por el Foro Económico Mundial que desde hace varios años viene publicando numerosos documentos y estudios sobre los ciber riesgos.

Cisnes negros, estrategias de diversificación inadecuadas, interdependencia o riesgo de contagio, y dificultad para evaluar el verdadero alcance de los riesgos, no son, por desgracia, elementos novedosos. Para aquellos familiarizados con las causas y desarrollo de las crisis financieras, las similitudes son evidentes

Una de las contribuciones más relevantes realizada por este organismo ha sido la elaboración del primer marco teórico para la definición de un modelo de cuantificación de ciber riesgos, publicado en enero de 2015. Este modelo se basa en lo que se ha denominado ciber valor en riesgo (CyberVaR) que no es otra cosa que la extensión del concepto de valor en riesgo a los riesgos de origen cibernético. El valor en riesgo es una métrica que tuvo su origen en el mundo financiero, y que actualmente es ampliamente conocida por el sector asegurador. A ello ha contribuido que marcos regulatorios como el de Solvencia II (o variaciones del mismo como el Tail-VaR utilizada en el caso del Swiss-Solvency-Test) hayan popularizado su utilización.

Aunque el Foro Económico Mundial no profundiza en detalles metodológicos, podemos asimilar el proceso para obtener el CyberVaR al utilizado para la determinación de cualquier VaR asociado a riesgos de origen financiero o de naturaleza aseguradora.

FIGURA 1.



Fuente: Foro Económico Mundial.

APLICACIÓN PRÁCTICA DEL MODELO DE CUANTIFICACIÓN DE CIBER RIESGOS

Este modelo de CyberVar impulsado por el Foro Económico Mundial es una herramienta extremadamente útil para la gestión de riesgos cibernéticos de cualquier organización. Es por ello que consideramos enormemente interesante profundizar en los aspectos teóricos de dicho modelo y, generalizando dicha metodología en base al marco conceptual definido, desarrollar una aplicación práctica para la cuantificación de ciber riesgos, que sea útil a cualquier organización a la hora de realizar una cuantificación económica de sus riesgos cibernéticos (Figura 2).

Identificación de los factores de riesgo

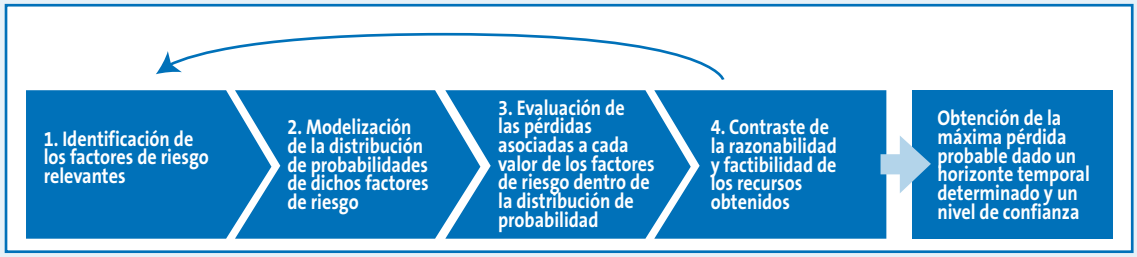
La complejidad y diversidad de los riesgos cibernéticos es tal que resulta impráctico asociarlos con variables económicas concretas (por ejemplo, los tipos de cambio o los movimientos de un índice de valores) como sucede con los riesgos de mercado o de crédito. En este aspecto, los riesgos cibernéticos se asemejan claramente a los de suscripción de la actividad aseguradora o a los operacionales.

Tanto en el caso de los riesgos de suscripción como especialmente en el de los riesgos operacionales es habitual partir de una modelización de **la frecuencia y severidad de los eventos de pérdida**. Vamos a seguir esta misma metodología.

Generalmente, la frecuencia es modelizada en función del volumen de exposición al riesgo, este nivel de exposición se puede considerar que, para el caso de los riesgos cibernéticos, depende de tres tipos de factores (Figura 3):

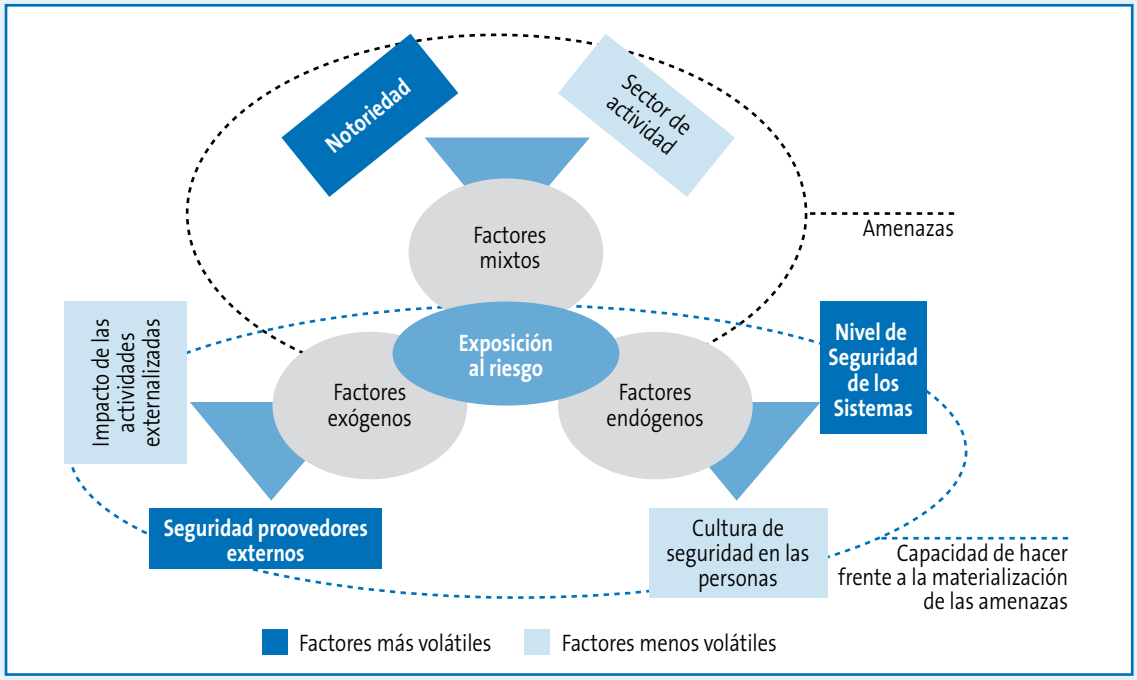
a) Factores endógenos de la Entidad.
b) Factores exógenos de la Entidad.
c) Factores mixtos.

FIGURA 2.



Fuente: Foro Económico Mundial.

FIGURA 3.



Fuente: Foro Económico Mundial.

Todos estos factores están relacionados tanto con el volumen de amenazas a las que tiene que hacer frente la organización, como con la capacidad de prevenir la materialización de dichas amenazas de forma directa o a través de sus proveedores clave.

Algunos de estos factores son especialmente dinámicos y, por tanto, requieren una reevaluación de forma más recurrente que otros. Un ejemplo práctico de ello puede ser el nivel de actualización de nuestros sistemas y antivirus, los cuales pueden convertirse en obsoletos de forma mucho más rápida que los conocimientos de las personas en nuestra organización. Respecto de la severidad existe una fuerte evidencia empírica sobre la relación de dicha variable con la resiliencia de la organización (y/o de los proveedores clave) frente a posibles contingencias de origen cibernético.

Es importante distinguir entre factores que permiten aumentar la resiliencia de la organización y los mecanismos de transferencia del riesgo que lo que producen es una disminución del impacto final de un riesgo al transferir todo o una parte de ese impacto a un tercero.

Modelización de las distribuciones de probabilidad de los factores de riesgo

Una vez identificados los factores de riesgo, el paso siguiente consiste en establecer las distribuciones de probabilidad a aplicar tanto a la frecuencia como a la severidad de los eventos de pérdida.

A la hora de ajustar una distribución a la frecuencia, hemos optado por la distribución de Poisson. Esta distribución es especialmente adecuada para modelizar aquellos sucesos dicotómicos con un elevado número de ensayos y una baja probabilidad de éxito. Este comportamiento refleja de manera razonable la naturaleza de los ciber riesgos caracterizados por un volumen elevado de intentos de ataque asociados a un número relativamente bajo de éxitos esperados.

El número de éxitos esperados (en este caso para un horizonte temporal de un año) coincide con el parámetro λ que caracteriza la distribución de Poisson y que debe ser ajustado en función de los factores de riesgo identificados en el epígrafe anterior. Un elemento importante a tener en consideración es la condición de independencia entre los diversos experimentos aleatorios que asumimos al optar por este tipo de distribución. Esta condición puede en principio resultar contradictoria con un fenómeno en el cual una misma vulnerabilidad pueden dar lugar a una pluralidad de "éxitos". Sin embargo, hemos de entender evento como el conjunto de pérdidas asociadas a una única vulnerabilidad, con independencia de las veces que la misma sea explotada.

En el caso de la severidad se ha optado por la distribución log-normal, en la medida que dicha distribución presenta una serie de características que la hacen útil para nuestros propósitos:

a) No puede tomar valores negativos
b) Es continua
c) Devuelve mayores probabilidades en los importes más bajos, es decir, es asimétrica positiva.

Todas estas características son coherentes con la limitada evidencia empírica de la que se dispone hasta el momento, aunque otras distribuciones similares podrían ser igualmente válidas. Lo que es importante en este caso, es que lo que se está modelizando es un indicador de severidad y no el importe de una pérdida. Dicha pérdida se determinará en el siguiente paso.

Una vez definidas las distribuciones de frecuencia y severidad será necesario introducir el concepto de escenarios. Cada escenario estará caracterizado por una distribución de frecuencia (que estará determinada por la exposición concreta al riesgo caracterizado por el escenario descrito) y una distribución de la potencial severidad del evento. A partir del informe de marzo de 2015 del gobierno del Reino Unido sobre ciber riesgos hemos definido los siguientes escenarios posibles. Todos ellos deben entenderse circunscritos a un origen cibernético:

a) Daños en los activos fijos o en las personas.
b) Daños en los sistemas, los datos o la propiedad intelectual que puedan ocasionar una pérdida de valor en los activos intangibles o una ineficacia en cualquier proceso de la organización distinto de la realización de su actividad comercial principal.
c) Costes derivados de una interrupción en la actividad comercial principal.
d) Costes derivados de la pérdida y/o difusión no autorizada de datos de carácter privado de terceros.
e) Fraude o extorsión.

Aunque teóricamente es posible asumir cierta correlación entre los escenarios a, b y c, así como entre d y e, se ha preferido considerar todos estos escenarios como independientes entre sí.

Evaluación de las pérdidas asociadas a cada valor de los factores de riesgo

Una vez definidos los distintos escenarios así como las distribuciones de frecuencia y severidad asociadas a dichos escenarios, el siguiente paso será realizar un número suficientemente alto de simulaciones a través de un proceso de Monte-Carlo. Cada una de estas simula-

ciones contendrá un número de eventos y la severidad asociada a cada uno de ellos.

A partir de esa información es posible proceder a la realización de una valoración de las pérdidas en las que se incurriría en cada simulación. Para ello es preciso tener en consideración una serie de aspectos:

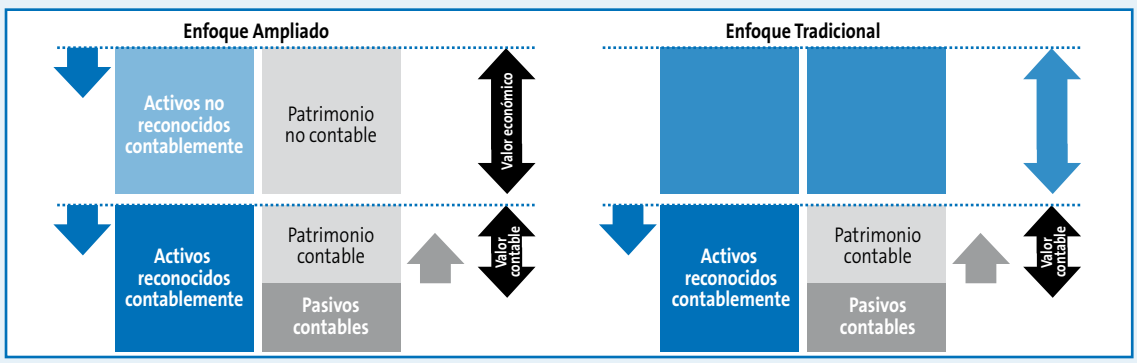
a) A efectos de gestión de riesgos y toma de decisiones, los potenciales impactos sobre elementos no reconocidos contablemente pueden ser extremadamente relevantes. Corresponderá, por tanto a cada organización evaluar en qué medida dichos elementos deben ser considerados (bajo un enfoque ampliado), o no, en la evaluación de las pérdidas asociadas a cada evento. Siempre teniendo en consideración que las situaciones de desequilibrio patrimonial vienen definidas legalmente bajo los estándares contables (Figura 4).

El enfoque ampliado será recomendable en aquellos casos en los que el valor económico de la organización es muy diferente del contable (por ejemplo, cuando existen importantes expectativas sobre beneficios futuros procedentes de propiedad intelectual o fondos de comercio autogenerados) y especialmente relevante para la toma de decisiones de gestión. En el resto de casos y en todo caso para evaluar en qué medida las pérdidas potenciales pueden implicar una situación patrimonial de desequilibrio, el enfoque tradicional es el que resulta adecuado. En nuestro caso hemos optado por seguir un enfoque tradicional.

b) Las pérdidas asociadas a cada evento están relacionadas con la severidad del mismo, no obstante, es importante tener en cuenta que es preciso estimar diversas tipologías de costes:

- Costes directamente variables en relación a la severidad del evento, tales como multas, indemnizaciones o costes de reparación de bases de datos o activos fijos. En este caso en cada escenario se realiza una transformación de la severidad a unidades afectadas (por ejemplo, registros con datos personales) siendo valorado el coste total en base a un coste unitario estimado.
- Costes de naturaleza semi-variable y que están relacionados con servicios necesarios para la resolución del incidente (por ejemplo, servicios forenses, asistencia jurídica, etc, etc..). Este tipo de servicios si bien pueden tener costes crecientes en función de la severidad del evento, tienden a distribuirse de forma escalonada. Nuestro modelo considera 3 niveles de costes semi-variables asociados a cada escenario, siendo el primer escalón equivalente a un coste nulo. De esta manera, el modelo recoge aquellos casos en los que parte de estos servicios se desempeñan en interno por la organización para eventos de baja severidad.
- Deterioro de valor de activos reconocidos en el balance (contable o económico en función del enfoque aplicado). Este importe se corresponderá con el deterioro que sería necesario practicar sobre el valor de aquellos activos afectados por la manifestación del riesgo modelizado. Este impacto se ha modelizado siguiendo un esquema similar al de los costes semi-variables. Para ello, se han establecido una serie de escalones de severidad del evento, asociados a diferentes porcentajes de deterioro en los activos expuestos. Al igual que en el caso anterior se ha considerado un primer escalón para aquellos eventos de baja severidad y donde se considera que no existe un impacto en el valor de los activos. Por otro lado, es importante tener presente que aquellas inversiones derivadas del evento de pérdida pero que puedan ser activadas (por ejemplo, la sustitución de un sistema de gestión inservible, y por tanto previamente deteriorado, por otro nuevo) no deberían ser tenidas en cuenta en el coste del evento en la medida en que su importe no supere el impacto del deterioro registrado.

FIGURA 4.



Fuente: Foro Económico Mundial.

c) Finalmente, en el caso de existir mecanismos de transferencia de riesgo (básicamente pólizas de seguro contratadas para cubrir algunos de los riesgos) será necesario tener en cuenta el efecto que dichos mecanismos tendrían en el coste de los eventos. En la medida de lo posible, es preferible no netear los importes de tal manera que se tenga visibilidad completa sobre los costes reales antes y después de hacer valer la póliza de seguro. En función de lo significativo que pueda ser el impacto de las pólizas de seguro será preciso considerar:

- Capitales máximos asegurados
- Importe de franquicias
- Potenciales costes de re-instalación de las primas al consumirse la cobertura

En nuestro modelo no hemos considerado la participación del Consorcio de Compensación de Seguros como consecuencia de un posible origen terrorista o de catástrofe natural de ninguno de los eventos de pérdida modelizados.

Contraste de la razonabilidad y factibilidad de los resultados obtenidos

Una vez realizado un número suficiente de simulaciones y valorada la pérdida asociada a cada una de ellas, deberá procederse a seleccionar el valor enésimo de pérdida mayor a partir del cual se determinará el Cyber-VaR.

De tal manera que si nuestro objetivo es, como sugiere el Foro Ecónomico Mundial obtener un VaR al 95% de confianza, deberemos por tanto considerar la pérdida situada en el percentil 95. Esto equivale para 1.000 simulaciones a tomar aquella que se sitúa en el lugar 950, de tal manera que existen 949 escenarios con pérdidas menores y solo 50 donde las pérdidas son mayores. Puede darse la situación de que las pérdidas situadas más allá de ese percentil sean muy superiores a la que sirve de punto de corte para el Cyber-VaR, en cuyo caso este importe puede no ser suficientemente informativo, se propone utilizar el valor promedio de esos escenarios o Tail-VaR para dichas situaciones.

El horizonte temporal a un año, supone desde un enfoque tradicional la métrica más habitual, ya que coincide con el plazo que suele discurrir entre dos cuentas anuales publicadas, documento a partir del cual se evalúan generalmente las potenciales situaciones de desequilibrio patrimonial. En enfoques ampliados podría tener sentido reducir este horizonte temporal (por ejemplo a un periodo trimestral) en cuyo caso la determinación del parámetro λ de frecuencia se vería igualmente afectada.

A la hora de realizar un contraste de las cifras obtenidas existen algunas técnicas útiles para realizar dicho contraste, se citan a continuación solamente algunas de las más habituales:

a) Benchmark: Mediante la comparación con otros indicadores sobre el valor económico del riesgo como pueda ser el coste de la cobertura de seguros, etc, etc...

b) Análisis de factibilidad cualitativa: Que consiste en comparar los resultados obtenidos mediante la modelización frente a análisis cualitativos desarrollados por personas con el suficiente conocimiento sobre los fenómenos modelizados.

c) Test de esfuerzo inverso: Que consiste en determinar a partir de los niveles de pérdida asociados al escenario CyberVaR el valor de las variables que dan lugar a dicho escenario y evaluar en qué medida son factibles o corresponden con una situación en el rango del nivel de confianza determinado (es decir si realmente se corresponden con el peor caso en 20 años, para el ejemplo del 95% de confianza estadística).

Una vez realizados los contrastes de razonabilidad y factibilidad sobre los resultados que se consideren necesarios, el paso siguiente será transformar la información obtenida en dichos contrastes en los ajustes sobre frecuencia, severidad y costes de cada uno de los escenarios, todo ello con el objetivo de ir refinando este proceso a lo largo de los diferentes ejercicios.

MÁS ALLÁ DE UN CYBER-VAR FINANCIERO, POSIBLES APROXIMACIONES REGULATORIAS.

Desde un punto de vista de toma de decisiones de gestión, un enfoque basado en el impacto financiero de los diversos riesgos es generalmente el más idóneo, ya que normalmente las decisiones en las organizaciones se toman siempre en función del impacto económico asociado a los mismas. Sin embargo, este enfoque pudiera no ser el más idóneo a efectos regulatorios. Si bien en los sectores financiero y asegurador, donde hasta ahora los capitales regulatorios han tenido un mayor desarrollo, ambas dimensiones, la operativa y regulatoria, son básicamente la misma, es decir la financiera, en el caso de servicios no financieros la dimensión sobre la que un regulador pudiera desear evaluar el valor en riesgo podría no ser de tipo financiero.

Si llegado el momento los servicios cibernéticos (o los energéticos, o sanitarios) fueran considerados como servicios lo suficientemente críticos como para ser sometidos a una regulación basada en valores en riesgo, es posible que la misma, más allá de unos requerimientos financieros (calculados conforme a un modelo como el presentado), impusiese unos requerimientos operacionales basados en pérdidas de operatividad máximas admisibles (Por ejemplo, número de días sin servicio, volumen de datos personales dañados, etc.) ya que en un contexto de economía interconectada puede ser tan dañina la quiebra operacional como la financiera.