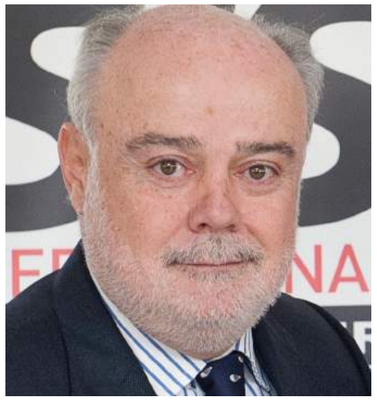
¿Buscando

un líder para el modelo?

D. Juan Muñoz Presidente de ASIS España



Juan Muñoz
CPP CSMP CSyP MBA
CEO Associated Projects
Presidente de ASIS España

CYBER

A lo largo de los últimos años varias funciones de las empresas han transformado su rol tradicional incrementado o extendiendo su importancia, convirtiéndose en transversales y/o estratégicas, o modificando su contenido como, por ejemplo, adoptando nuevos modelos de gestión.

Entre los primeros, está el caso de las **finanzas.** Cuando pasaron a ser transversales, se introdujo la figura del controler y la gestión de tesorería pasó a tener un papel prioritario. También el de la función **legal. C**uando pasó a ser transversal y se adoptó el formato anglosajón donde todos los procesos y decisiones adoptan una perspectiva legal y por lo tanto deben ser revisados bajo los criterios de esta. En ambos casos este enfoque permanece si cabe con mayor autoridad todavía.

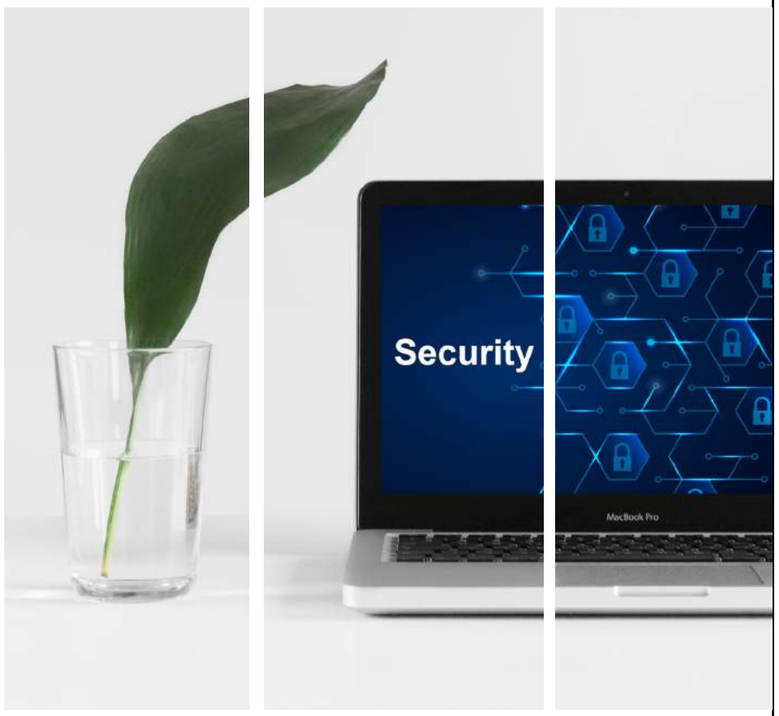
En el segundo grupo podemos incluir la evolución de la función de personal hacia la de **recursos humanos**, que en algunos casos es cierto que sólo es semántica; y la de los **seguros hacia la gerencia de riesgos,** que lo es también en muchos otros. Esta es una realidad dado que la gerencia de riesgos es un proceso complejo donde la transferencia financiera ocupa una de las últimas fases, aunque no por ello menos importante. En este contexto se puede situar también la **seguridad corporativa** en su largo camino desde proteger activos físicos a hacerlo con estos y además con los activos intangibles hasta su componente actual de valor añadido.

En un paso más adelante, ahora estamos en pleno proceso de adaptación hacia el marco de **la ESRM (Enterprise Risk Security Management).**

Resulta difícil no reconocer que desde hace unos años ha aparecido un nuevo driver o impulsor en el entorno empresarial, que se ha convertido en estratégico, pero cuya complejidad merece una reflexión. Y este no es otro que la gestión holística del riesgo en un nuevo horizonte, que por el momento es policéfala y que todo parece indicar que no va a poder continuar siéndolo por mucho tiempo. Y es que esta nueva gestión de riesgos (incluyendo los seguros, pero ni mucho menos limitados a éstos) es ahora una función estratégica responsabilidad del más alto nivel de las organizaciones. **Los riesgos derivados de la información**, a través de los sistemas de información o más allá de estos, con especial énfasis en la llamada ciberseguridad; **los riesgos derivados del cumplimiento normativo,** presionados por la responsabilidad penal de las personas jurídicas, por ejemplo con el Deber de Protección (Duty of Care); o los amplios **riesgos de seguridad derivados de la globalización**, como la delincuencia violenta, el terrorismo o el crimen organizado, han tejido una red compleja de riesgos que han vuelto a constituirse en un arquitectura de silos, lo que precisamente trataba de evitar el ERM.

Y con ellos han renacido o surgido las posiciones que dirigen las **diferentes áreas de gestión de estos riesgos.** Por un lado, los CROs (Chief Risks Officers), con un perfil combinado en gran medida de economistas y abogados; por

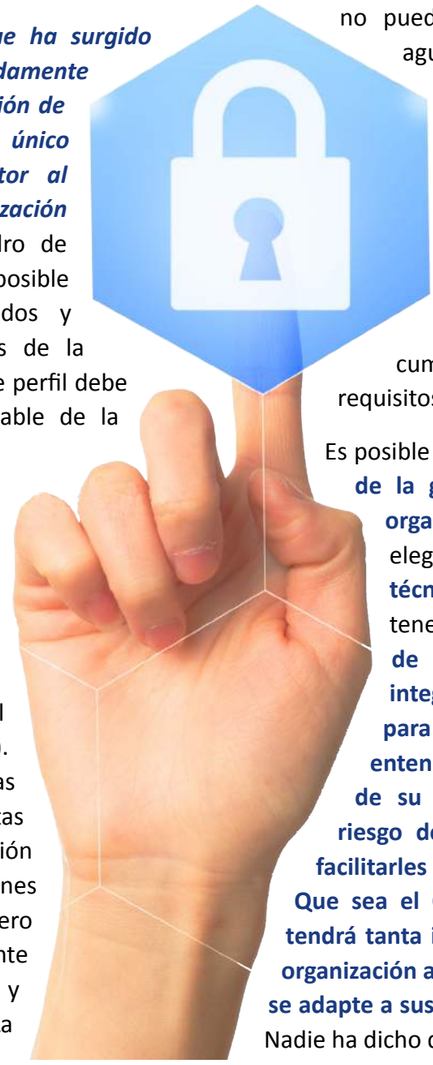
otro, los CIOs y CISOs (Chief Information Officer y Chief Information Security Officer) e incluso los más recientes DPOs (Data Protection Officer), con un perfil fundamentalmente técnico y en el último caso legal; también los **CSOs (Chief Security Officers),** muchos procedentes de las fuerzas armadas, de las fuerzas de seguridad del estado y ahora también de los servicios de inteligencia; y, por último, los recientemente aparecidos CCO (Chief Compliance Officer), con un fuerte componente legal. Quién considere que el modelo no es complejo y confuso, que levante la mano.



Si partimos de la base que la llamada *C-Suite está formada por el pequeño grupo de directivos senior que dirigen una organización* podríamos encontrarnos con una situación excepcional cuando en un escenario hipotético ocho o diez de los miembros de un comité de dirección (CEO, CFO, COO, CLO y alguno otro), cuatro o cinco estén enfocados a la gestión de riesgos. Si esperamos que las organizaciones van a aceptar esta solución policéfala podríamos estar equivocados y de hecho estas ya han comenzado a tomar decisiones. En primer lugar, un chief es una persona del máximo nivel en una organización que reporta directamente a la cabeza de esta. Es decir que no todos los responsables de sistemas de información, por ejemplo, son CIOs ni CISOs ni todos los responsables de seguridad corporativa – o como ahora se denomina seguridad organizacional – son CSO. De hecho, sucede todo lo contrario, representan una minoría. No es problema semántico, sino de autoridad.

Las primeras medidas han venido por las llamadas convergencias. La primera convergencia que afecta a la seguridad lógica y a la seguridad corporativa (que algunos llaman también seguridad física limitando su naturaleza real). No es un secreto que su aplicación real está siendo más compleja de lo esperado y progresa poco a poco no sin haber descubierto ciertas tensiones de poder dentro de las organizaciones. Sin embargo, en una reciente conferencia presentada por un consultor de una de las Big Four, este comentada que la compleja gestión de riesgos actual requería una única cabeza o un comité de gestión, que a su vez también requería una cabeza visible. Y al ser preguntado sobre el perfil concreto contesto que en muchos de los casos actuales el liderazgo del modelo había sido asumido por los responsables de seguridad corporativa debido a diferentes factores. Por ejemplo, en el caso de las infraestructuras críticas, muy influenciadas por el factor regulatorio. Ahora aparece en el horizonte la segunda convergencia, que extiende la primera a la gestión de riesgos convencional y a la continuidad de negocio.

Lo que está claro es que ha surgido una nuevo y extremadamente complejo modelo de gestión de riesgos que requiere un único responsable o interlocutor al máximo nivel de la organización y el diseño de un cuadro de mando lo más sencillo posible que refleje y mida todos y cada uno de los riesgos de la organización. ¿Qué tipo de perfil debe tener ese súper responsable de la gestión de riesgos?



En 2004 ASIS International, la organización líder mundial en seguridad corporativa, creo el perfil del Chief Security Officer que en 2010 se convirtió en un estándar internacional (ANSI/ASIS CSO.1-2013). Este recoge no solo las áreas de responsabilidad directas e indirectas de esta posición como también sus misiones y responsabilidades. Pero quizás lo más interesante sean las capacidades y habilidades deseadas. La mayoría de ellas no son técnicas sino de gestión y liderazgo y la realidad es que son ajenas o no habituales al prototipo de profesional que ocupa habitualmente estas posiciones. Por ejemplo, enfoque al cliente, agilidad organizacional, resolución de problemas, capacidad de escuchar, agilidad estratégica, calidad en las decisiones, coraje de gestión y algunos otros, como capacidades interpersonales o enfoque hacia el riesgo, sin el cual las organizaciones no pueden sobrevivir. El papel lo aguante todo y el documento parece una lista de deseos imposibles de alcanzar o acumular en una sola persona. Como aquel especialista en selección de ejecutivos que me pregunto si habíamos encontrado alguien que cumpliera muchos de los requisitos porque ellos no.

Es posible que el **máximo responsable de la gestión de riesgos de una organización**, uno sólo, sea elegido no por sus **capacidades técnicas** solventes, que deberá tener, sino por sus **habilidades de comunicación, liderazgo e integración, y por su capacidad para traducir a un lenguaje entendible a los máximos niveles de su dirección el escenario de riesgo de una organización y para facilitarles la toma de decisiones. Que sea el CRO, el CISO o el CSO no tendrá tanta importancia dado que cada organización adoptará la fórmula que más se adapte a sus condiciones y necesidades.** Nadie ha dicho que esto sea fácil.

Factor de Visibilidad

Un indicador cuantitativo para valorar el riesgo del proyecto

D. Fernando Vegas-Fernández Ingeniero de Caminos
D. Fernando Rodríguez López PhD Msc Civil Engineer

Fernando Vegas-Fernández
Ingeniero de Caminos
Investigador en la Universidad Politécnica de Madrid
ETSICCP

Fernando Rodríguez López
PhD Msc Civil Engineer
Profesor titular. Universidad Politécnica de Madrid
ETSICCP

VISIBILIDAD

El Factor de Visibilidad es un indicador cuantitativo del nivel de riesgo que, además, posibilita la combinación de varios eventos de riesgo obteniendo un único evento resumen, con impacto y probabilidad propios.

El informe de riesgos de un proyecto puede tener más de 40 páginas, describiendo entre 30 y 300 riesgos agrupados en capítulos dentro de hasta 11 matrices de riesgos (1). Sería deseable poder resumir su nivel de riesgo con un simple indicador numérico, al igual que se hace con el riesgo de aludes, oleaje o viento, evitando la necesidad de leer el informe entero para saber si la situación es relevante o no.

Doble reto: por un lado, se requiere cuantificar riesgos de distinta naturaleza (coste, plazo, reputación, seguridad, salud, calidad o mixto); por otro lado, es necesario resumir varios eventos de riesgo definidos por sus impactos y probabilidades, mediante un único evento equivalente.

Los indicadores usuales suelen estar orientados a tipos de riesgo concretos, específicos de cada negocio. El producto impacto por probabilidad proporciona un resultado numérico que es poco intuitivo y no resulta eficiente para combinar riesgos. **El coste,** siendo el indicador más evidente, no siempre es calculable (por ejemplo, en riesgos reputacionales o que afecten al cliente) y, además, no es significativo por sí mismo si no se compara con el presupuesto de venta del proyecto. Por otra parte, la combinación de dos o más eventos de riesgo obteniendo un impacto y probabilidad equivalentes escapa a las posibilidades del análisis de riesgos conocidas hasta ahora.

El Factor de Visibilidad es una función matemática que convierte las evaluaciones cualitativas de impacto y probabilidad de cada riesgo en un indicador numérico, lineal de 0 a 100 (2).

Para ello se realiza una interpretación numérica previa de los impactos y probabilidades usando escalas de Likert y, con estos valores, se calcula el Factor de Visibilidad. Esto posibilita valorar cada uno de los riesgos y **destacar los más graves**; dándoles visibilidad (gráfico 1)

Con este novedoso indicador se puede dibujar en un mapa de calor curvas de nivel de riesgo que facilitan la comprensión inmediata de la relevancia de los eventos de riesgo existentes.

Pero incluso con esta mejora todavía no se conocería cuál es el nivel de riesgo de cada matriz, ni el global del proyecto. Por eso, basado en el Factor de Visibilidad, se ha definido un método de combinación para calcular un evento de riesgo equivalente a un escenario dado, con su propio impacto y probabilidad (2).

De esta forma, sería posible describir el riesgo global del proyecto mediante su Factor de Visibilidad y su impacto y probabilidad equivalentes.

Gráfico 1

Factor de visibilidad: eventos de riesgo por capítulos y matrices