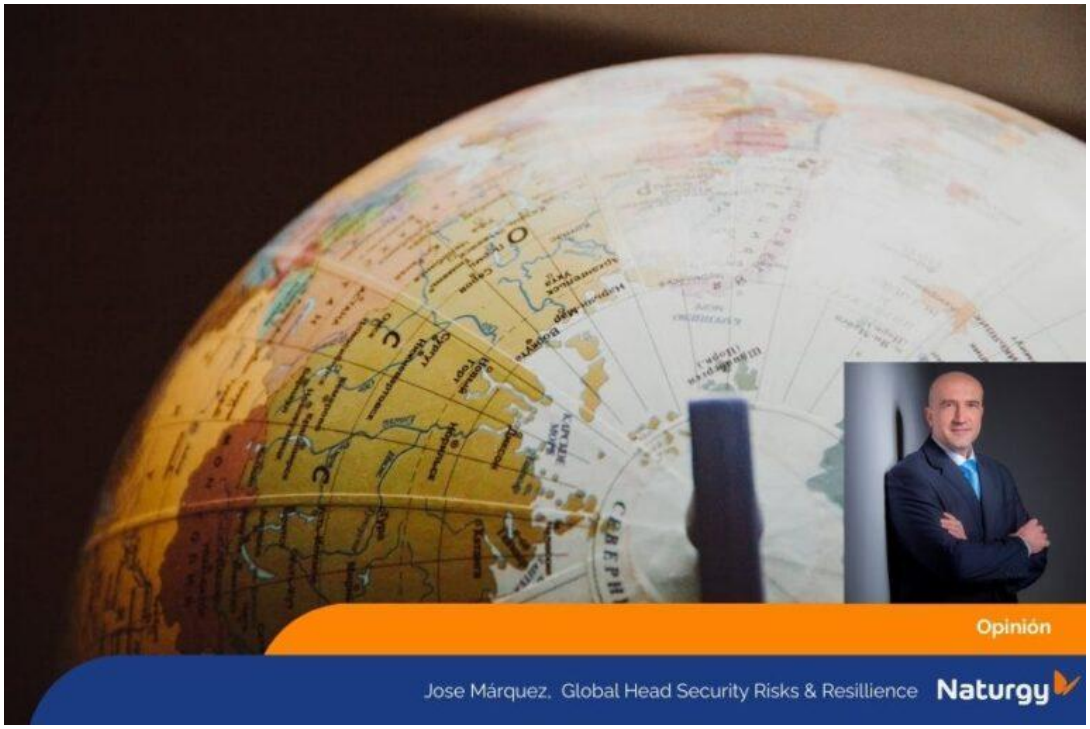


- 6 marzo 2026

Noticias, Artículos de opinión

RIESGOS Y SEGURIDAD: DOS MUNDOS QUE POR FIN DEBEN HABLAR EL MISMO IDIOMA

Los últimos episodios geopolíticos, caídas masivas de servicios esenciales y ciberataques masivos han demostrado que los riesgos no se limitan al plano financiero o reputacional: también amenazan la continuidad operativa. La Unión Europea, consciente de ello, ha impulsado las directivas CER y NIS 2, que unen riesgo empresarial y seguridad, exigiendo integrar en su gestión no solo la prevención, sino también planes de respuesta ante incidentes graves que afecten a los servicios esenciales. Pero esto no sólo aplica a las grandes empresas, sino también a las PYMES que forman parte de la cadena de suministro estratégica.

1. El papel de los departamentos de riesgos y seguridad en la empresa actual

Durante algún tiempo, los departamentos de riesgos y seguridad —entendido este último en su acepción anglosajona "security"— fueron vistos como los "aguafiestas" del negocio: los que ponían límites, los que decían "no" a algunos proyectos por prudencia. Hoy, ese papel ha cambiado. En un entorno donde lo imprevisible se ha convertido en

rutina, los responsables de riesgos y seguridad son arquitectos de resiliencia.

Todos damos por hecho que la gestión del riesgo no consiste en rellenar matrices o calcular probabilidades. Se trata de entender cómo una crisis puede afectar a la reputación, a la continuidad o a la confianza de los clientes. El riesgo bien gestionado no frena el negocio: lo hace más inteligente.

Cada vez más, ese papel estratégico se confunde con otro emergente: el de la resiliencia. No basta con anticipar; hay que resistir, recuperarse y adaptarse. Quizá el futuro no pase por tener un *Chief Risk Officer* —gestión tradicional del riesgo— y por otro lado un *Resilience Lead* —responsable de los planes de gestión de crisis y de continuidad de negocio—, sino por un Chief Resilience Officer que gobierne ambas funciones bajo un mismo propósito: mantener la empresa viva ante lo inesperado.

2. La seguridad dentro de Enterprise Risk Management

Durante décadas, la gestión de seguridad se movió en su propio mundo: protocolos, accesos, cámaras, vigilantes de seguridad. Cumplía su función, sí, pero sin conexión real con la estrategia.

Integrarla dentro del marco de Enterprise Risk Management (ERM) significa colocarla donde siempre debió estar: en el corazón del negocio. La seguridad no solo protege, también previene, informa y anticipa. Ayuda a traducir las amenazas en inteligencia para la toma decisiones.

Porque no hay resiliencia sin seguridad. No hay continuidad sin protección. Y no hay futuro sin confianza. Integrar ambas funciones es dejar de hablar de "costes" y empezar a hablar de valor. Es por ello que la mayor organización internacional de líderes de seguridad (ASIS International) ha impulsado el estándar ESRM (Enterprise Security Risk Management).

3. Retos de la integración

Lograrlo no es tan sencillo. Riesgos y Seguridad hablan dialectos distintos dentro de la misma empresa. Uno se mueve entre métricas y matrices; el otro entre personas, activos y tecnología. Los primeros piensan en impactos; los segundos, en incidentes.

El reto está en encontrar un idioma común. En muchas organizaciones, aún persisten silos, jerarquías rígidas y cierta desconfianza mutua. La seguridad teme diluirse entre números; riesgos, perder control sobre lo técnico.

Además, el entorno no ayuda. Los riesgos ya no son lineales ni previsibles: un fallo de ciberseguridad puede causar un daño reputacional, un corte eléctrico puede derivar en una crisis social, una disrupción geopolítica (como la que estamos viviendo en medio oriente) puede paralizar la cadena de suministro. Todo está conectado, pero no siempre lo están los equipos que deberían gestionarlo.

4. Beneficios para la organización

Cuando la integración se logra, el cambio se nota. Las decisiones se vuelven más coherentes, las crisis menos caóticas y los recursos mejor aprovechados.

Integrar seguridad a través de ESRM ofrece tres grandes beneficios:

- **Primero, una visión 360º del riesgo. La seguridad aporta inteligencia de campo, conocimiento operativo y capacidad de respuesta que complementa la visión estratégica del riesgo.**
- **Segundo, una cultura de resiliencia real, donde los empleados entienden que proteger es parte de su trabajo, no solo una tarea del departamento de seguridad. La cultura de resiliencia es la mejor vacuna contra la incertidumbre en este entorno BANI.**
- **Y tercero, una empresa más creíble ante clientes, reguladores y accionistas, porque demuestra que su discurso sobre sostenibilidad o cumplimiento se traduce en hechos concretos.**

La seguridad no es un muro que separa; es el puente que conecta prevención, respuesta y confianza.

5. Evolución futura en un entorno digital y complejo

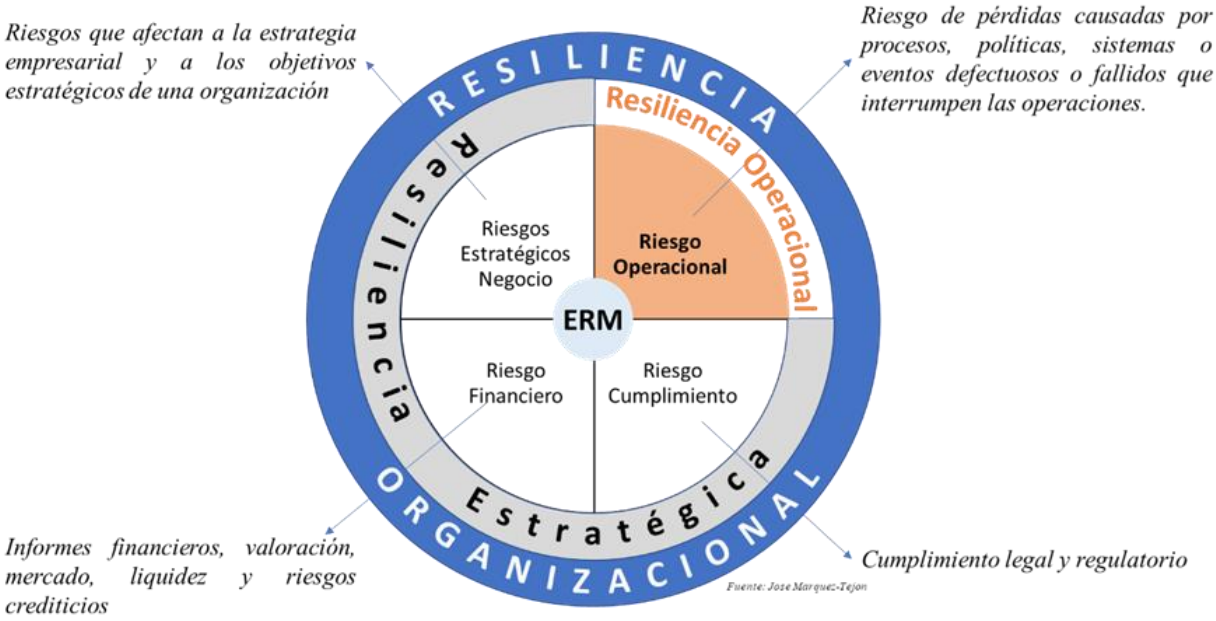
Todo indica que la convergencia entre riesgos y seguridad será irreversible. En el futuro, las fronteras entre lo físico y lo digital se difuminarán: la seguridad de los datos será casi tan importante como la de las personas, y las amenazas híbridas requerirán respuestas unificadas.

La gobernanza también evolucionará. Los criterios ESG y las exigencias regulatorias impulsarán un modelo donde la seguridad y la defensa sean un valor social, visible y medible. Las empresas deberán demostrar que protegen no solo su beneficio, sino también a sus empleados, comunidades y entorno.

Y en la cúspide de este cambio aparecerá una nueva figura: el Chief Resilience Officer, heredero del gestor de riesgos tradicional y del gestor de los planes de respuesta. Un perfil que combine estrategia, tecnología y humanidad; que no tema al cambio, sino que lo anticipe.

La integración entre riesgos y seguridad no es una tendencia, es una necesidad. Las empresas que lo entiendan a tiempo serán más ágiles, confiables y sostenibles. Las que sigan gestionando ambos mundos por separado, simplemente, llegarán tarde.

En definitiva, el riesgo bien entendido y la seguridad bien integrada no son un gasto: son la mejor inversión para garantizar el futuro.



Fuente: Márquez Tejón, J. A. (2024). La contribución estratégica de la función corporativa de security en la resiliencia organizacional: un estudio empírico en sociedades cotizadas que operan en España.