Seguridad pública y privada: reflexiones acerca de la metodología en el análisis y la gestión del riesgo

José Luis Hernangómez de Mateo [*]

Tema: Se analiza el concepto de análisis de riesgo en seguridad tanto para el ámbito público como el privado, y se determina la necesidad de metodologías convergentes y de herramientas que permitan la gestión global de los riesgos.

Resumen: La "transversalidad" entre las amenazas y los activos a proteger en la esfera pública y privada obliga a desarrollar metodologías que integren todas las disciplinas de la seguridad de un modo realmente convergente, tratando de considerar de forma real y efectiva a la seguridad como un todo y superando la conocida coordinación, buena pero insuficiente, de diferentes metodologías y sistemas de gestión. En este ARI se repasa el contexto de seguridad en el que operan los Estados y las empresas, y se dibuja de forma comprehensiva un esquema metodológico e instrumental que contribuiría a una protección adecuada de los activos, en alineación con los fines últimos de entidades públicas y privadas. Finalmente se formulan algunos criterios de aproximación.

Análisis:

Introducción

Vivimos en un entorno cambiante y globalizado. Desde el punto de vista de la seguridad global, y por tanto de la gestión del riesgo, el entorno es además hostil, tanto para las instituciones públicas como las privadas. Los Estados tienen sus intereses y, aunque en ocasiones sean compartidos, la razón de Estado a veces prevalece sobre ese espacio común. Bien se trate de países tradicionalmente hostiles, bien de socios o aliados, lo cierto es que los Estados tienen intereses en su territorio y en el de la competencia o aparentemente neutral, y que dichos intereses se hallan expuestos a riesgos originados y presentes en todas las ubicaciones posibles, incluido el ciberespacio. En el ámbito privado ocurre algo parecido: las empresas, y en especial las grandes corporaciones, tienen sus activos repartidos por todo el mundo, expuestos a todo tipo de amenazas, algunas de ellas derivadas de la propia movilidad de dichos activos y amenazas. El enfrentamiento de un catálogo de amenazas llamémosle tradicional con el repertorio de activos que hoy día Estados y compañías poseen en todo el mundo, convierte la gestión de la seguridad global en un auténtico reto.

Hoy día, esa "multinacionalidad" de las amenazas se combina con la de los activos, obligando a realizar un análisis más complejo que los ya de por sí complicados análisis sectoriales centrados en los sistemas de información, en los bienes inmuebles,

[*] *Director de Planificación y Alertas del Grupo Prisa, doctor en Ciencias Políticas y Sociología, coronel en situación de reserva, especialista en Investigación Operativa, director de Seguridad y auditor SGSI, con una acreditada experiencia en inteligencia.*

medioambiente incluido, o en aquellos intangibles cada vez más determinantes en la sociedad de la comunicación y de la percepción en que vivimos. Las dependencias entre amenazas y activos son elementos de estudio obligado en un mundo en el que las fronteras de todo tipo son muy difusas. La denegación de servicio en un sistema de información posiblemente comience con una intrusión, y no necesariamente informática. Un fallo en el control de accesos físicos de una compañía puede provocar una fuga de información en soporte papel o digital, tan dañina a efectos de confidencialidad como la que tendría lugar mediante un "troyano" introducido por un *hacker*. Un centro de proceso de datos debe ser un área tan segura como el vehículo que transporta habitualmente al consejero delegado de una gran corporación. Hay muchas clases de soportes de información vital para la empresa, y todos precisan una protección eficaz para garantizar la confidencialidad, la integridad y la disponibilidad de esa información.

En estos tiempos en los que la piratería en el Océano Índico campa por sus respetos y pone en jaque a la seguridad global de los Estados, estamos viendo cómo cualquier empleado de cualquier compañía, y no necesariamente de alto nivel jerárquico, puede convertirse en un grave problema de seguridad. La probabilidad de que una amenaza se materialice aprovechando la vulnerabilidad de toda persona, no es cuestión de nómina. El caso de la piratería en el Índico es muy ilustrativo de la relatividad de los enfoques tradicionales: el secuestro de unos empleados y de unos activos pertenecientes a una empresa privada se convierte en toda una crisis para un Estado. Entonces… ¿dónde comienza y termina la privacidad de los activos, al menos en cuestión de su seguridad?

Hoy día, en un análisis de riesgo global hay que prestar atención a muchas variables. Tengamos presente que la criticidad de un activo no deriva sólo de su estatus, sino de sus dependencias con relación a los demás, sean de la empresa o del Estado. Dejemos la piratería marítima y pensemos en las infraestructuras críticas de un Estado: en centrales energéticas, mercados financieros, centrales de telecomunicaciones y de transporte como aeropuertos, estaciones de metro y terminales de trenes y autobuses, centrales de control y distribución de agua, gas y electricidad, refinerías de petróleo… El 80% de ellas son de titularidad privada.[1] Entonces, ¿a quién compete su seguridad? Sin duda, al ámbito privado y también al público. La gestión global de intereses obliga a la gestión global de los riesgos para lograr también una seguridad realmente global.

El mundo público y privado necesitan de gestiones sinérgicas. Las empresas y los Estados, los activos y las amenazas, las nuevas tecnologías y la diversificación de mercados… se benefician de oportunidades globalizadas y también abren nuevos frentes que proteger. Los avances tecnológicos han propiciado más herramientas de trabajo, pero también un grado de incertidumbre añadido. Los actores públicos y privados deben dotarse de una armadura eficaz que les permita operar en ambientes de incertidumbre con el mayor grado posible de seguridad. El entorno cambiante, globalizado y hostil tiene capacidad de explotar vulnerabilidades, provocando situaciones de crisis y de emergencia. Es imperativa la convergencia entre actores, entre disciplinas, ente metodologías y entre herramientas.

El entorno de seguridad

Los catálogos tradicionales de amenazas deben ser revisados a la luz de la vida actual. Los actores públicos y privados se hayan sujetos a amenazas que, según qué activo y sus particulares circunstancias, se traducirán en un riesgo mayor o menor.

[1] Centro Nacional de Protección de Infraestructuras Críticas, http://www.arcert.gob.ar/10_aniv/presentaciones/proteccion_infraestructuras_criticas_espana.pdf (16/XI/2009).

Tanto el Estado como las empresas se hallan bajo la exposición de estos vectores de seguridad:

- Las agresiones de todo tipo contra el personal, tenga el nivel que tenga en la empresa o en la institución, como el asesinato, el secuestro, la extorsión y el chantaje, todas enfocadas en la libertad personal, con origen en la delincuencia común, el terrorismo o el crimen organizado.

- La competencia con otras empresas o con otros Estados, en especial las actividades de Inteligencia, y en general la actuación lesiva para los intereses propios desde terceras partes (competidores, proveedores, clientes, accionistas, socios, aliados críticos…).

- Con independencia del grado de sofisticación tecnológica pública o privada, actividades voluntarias y fortuitas, internas y externas, dirigidas contra instalaciones y soportes de información, sean tecnológicos o no, que supongan pérdida o destrucción de información; aquí entran las acciones de *hacking amateur* y profesional, y la adquisición o mantenimiento inapropiados de medios tecnológicos que almacenan, procesan y trasvasan la información.

- Las perturbaciones de índole social, política y económica de aquellas regiones de interés actual y futuro.

- La conflictividad laboral vinculada a los recursos humanos durante el ciclo completo de la vida laboral de todo empleado, con independencia de su nivel, es una amenaza clave y ejemplo del carácter transversal de la seguridad.

- Las operaciones esenciales vinculadas al mantenimiento de las instalaciones y de sus contenidos son críticas, y no deben permanecer ajenas a las consideraciones de seguridad.

- Las acciones delictivas dirigidas contra bienes en forma de atracos, robos, hurtos, fraudes, falsificaciones de moneda o de información, e incluso el vandalismo.

- Las acciones de la naturaleza, unas más previsibles que otras: incendios, catástrofes y otros acontecimientos que puedan originar destrucciones o inhabilitaciones masivas de forma temporal o permanente de todo tipo de recursos. Piénsese en la pandemia de gripe actual y en su agresividad simplemente en términos de capacidad de contagio como causa de ausencias laborales prolongadas en procesos críticos para toda organización, sea pública o privada.

- Las actividades voluntarias o fortuitas, provenientes del interior o del exterior del ámbito a proteger, que puedan constituir una agresión al medioambiente.

- Las actuaciones específicas o generales que puedan afectar al valor cada vez mayor de los activos intangibles (credibilidad, reputación, solvencia de la marca…), originando daños severos o irreparables. Las entidades públicas y privadas, en materia de seguridad global, deben actuar con sentido de la

responsabilidad social, cuestión de especial relevancia y con influencia creciente en todo resultado final.

Que el Estado o una empresa sea capaz de afrontar con éxito la gestión de riesgos exige, por tanto, conocerse muy bien a sí mismo y conocer muy bien el entorno donde opera. Esto significa ser capaz de mirar hacia dentro, de vigilar el perímetro –cada vez más difuso– y también de observar y analizar lo que ocurre al otro lado.

Una metodología

Todo está inventado. O casi todo, porque una relectura de lo mucho escrito sobre gestión de riesgos permite hacerse una composición acerca de lo que hay, del *gap* existente con las necesidades actuales y del camino a recorrer en la dirección adecuada. La dirección adecuada… ¿para qué? Para poder realizar un análisis de riesgos realmente convergente y global.

El objetivo último de toda metodología de seguridad es múltiple: concienciar a los responsables de la seguridad (la alta dirección de una empresa, los gobiernos) y a los responsables directos de los activos acerca de la existencia de riesgos y la necesidad de proteger aquéllos; disponer de un marco teórico y sistemático que permita detectar amenazas, activos y riesgos asociados, para poder evitar o mitigar sus efectos; final y opcionalmente, lograr certificaciones que acrediten un nivel aceptable de seguridad de la organización o del proceso en cuestión.

El abanico de disciplinas de seguridad es enorme, y algunas de ellas son auténticas decanas en el *campus* de la seguridad. Todas utilizan un repertorio más o menos extenso de metodologías, en la mayor parte de los casos adaptadas a los riesgos que pretenden gestionar. En unos casos, se centran más en las amenazas y, en otros, sobre los activos. Por esta razón, encontrar una metodología de amplio espectro que permita conjugar amenazas y activos de muy diversa índole no es sencillo. Pero no imposible.

Desde hace años existe un esfuerzo fructífero por estandarizar tanto terminología como el método en el ámbito de la seguridad de la información, eso sí, centrado en la información soportada por sistemas tecnológicos. Existen iniciativas privadas tendentes a aprovechar esa metodología sistemática recogida en las normas ISO de la serie 27000, de modo que los dominios, objetivos de control y controles de seguridad no se refieran exclusivamente a la seguridad de la información contenida en soportes tecnológicos, sino a la seguridad global de todo tipo de activo en una corporación o institución cualquiera, pública o privada.

Algo hemos apuntado anteriormente en este sentido. En el mundo privado, el de la empresa, hablamos de activos no sólo de información, también la reputación, la libertad de un empleado, el proceso de consolidación financiera, el control de acceso al edificio, la confidencialidad en la prestación de un servicio… son activos a proteger. En el mundo público, en el del Estado y de la Administración, la reputación de una empresa o de un sector estratégico, la libertad de actuación de su tejido industrial, la consolidación en mercados de interés, la información operativa y de alto nivel de los departamentos ministeriales y la confidencialidad en el intercambio de información también son activos. Todo lo anterior apunta a una vía, sólo a una de las posibles, pero cuyo rigor metodológico parece haber sido contrastado en lo particular mediante procesos certificadores reconocidos internacionalmente.

Dicho todo esto, creemos que una metodología global adecuada para el análisis de riesgos de todo tipo, utilizable por entidades privadas y públicas, incluido el mismo Estado como tal, debería reunir las siguientes características e incluir los pasos que se citan:

- Adoptar una terminología común, sujeta a los estándares y al reconocimiento internacional, como es el caso de la Organización Internacional para la Estandarización (ISO).

- Incorporar el conocido ciclo de Demming, también conocido como PDCA (*Plan, Do, Check, Act*), es decir, planificar, hacer, verificar y corregir. Este ciclo lo conocen muy bien cuantos llevan años trabajando en el ámbito de la seguridad con criterios de calidad. En la fase de planificación se identifican los riesgos, se cuantifica cada uno de ellos en función de su probabilidad de ocurrencia y del impacto que supondría su materialización, y se identifican las acciones apropiadas para reducir los riesgos a un nivel aceptable. En la fase de ejecución se implementan las medidas, también conocidas como contramedidas, para mitigar los riesgos, y se conciencia al personal mediante acciones de divulgación y formación. En la fase de control se supervisa que se adoptan las medidas resultantes del análisis y la eficiencia de su aplicación. Finalmente, en la etapa de corrección, se ajusta si es preciso el plan de adopción de medidas a la luz de nuevos análisis de riesgos tras la implantación de las medidas de seguridad. Todo el proceso deberá ser documentado.

- Determinar con claridad el negocio. Conocer el negocio significa, para una empresa, disponer de inteligencia sobre el sector y sobre la propia empresa (su historia, su situación actual, sus propietarios, sus directivos y aquellas terceras partes críticas y fundamentales, sus productos, su mercado, su idiosincrasia…). Para un Estado, significa conocer su historia y las circunstancias internas y externas que le llevan a la situación actual, sus actores principales, sus líderes actuales y las relaciones entre otras Administraciones y otros Estados, socios, aliados o rivales. Simple y llanamente, se trata de conocer en profundidad lo que se quiere proteger y su entorno inmediato. Todo ello facilitará la posterior identificación concreta de activos a proteger y la determinación de una estrategia de comunicación de seguridad adecuada.

- Identificar los activos y sus dependencias. Esto supone aumentar el grado de detalle en el conocimiento, concretando cuáles son los intereses de todo tipo a proteger de cualquier amenaza externa o interna. La identificación debe incluir los activos tangibles (personas, instalaciones, recursos de producción y medios en general) e intangibles (procesos, marca, reputación, confianza...). Una empresa deberá poner el acento en sus directivos y empleados críticos por la relevancia de su trabajo o por las condiciones en que realizan sus funciones, los locales que utilicen como oficinas, centros de producción, almacenaje o distribución, las áreas seguras –como centros de proceso de datos, de dirección y, en general, donde pueda existir valores como la información confidencial en cualquier soporte–, las dependencias entre dichos activos, pues por lo general cada activo está vinculado a otros, y el riesgo sobre uno puede suponer la afectación de otro… También protegerá sus procesos para evitar el fraude, la fuga de información, la interrupción de tareas críticas, la reputación o la credibilidad de la empresa y de sus productos o servicios. El Estado igualmente debe confeccionar un catálogo de activos con sus dependencias. Ese catálogo deberá estar constituido no sólo por

activos de titularidad estatal, ya que el tejido nacional está integrado por entidades privadas, desde ciudadanos individuales hasta las grandes corporaciones, todos ellos contribuyentes de las arcas públicas.

- Identificar amenazas. Conocer el negocio y su entorno es un factor determinante a la hora de poder elaborar una relación de fuentes de peligro para los activos, incluyendo su forma de actuar y de las vías por las que podrían acceder a los activos a proteger. Debe ser posible realizar un catálogo general de amenazas lo suficientemente amplio como para que aplique a todo tipo de institución pública o privada que proteger, y que permita la progresiva sustitución de catálogos sectoriales, cuya gestión de forma convergente resulta compleja incluso bajo la guía de estándares como la PAS 99.[2]

- Atender a la "multinacionalidad" de los activos y de las amenazas. Hoy día, pueden llegarse a materializar amenazas puntuales o transnacionales, como el narcotráfico, el crimen organizado, el terrorismo, redes de fraude… provenientes de multitud de focos y de ubicaciones geográficas diferentes sobre activos de una empresa o de un Estado diseminados por todo el mundo, el espacio incluido. No olvidemos que las amenazas pueden actuar desde el exterior de la entidad que trata de proteger sus activos, pero también pueden aprovechar vulnerabilidades internas: procesos defectuosos de producción o de reorganización, personal con una cualificación deficiente o descontento de su situación laboral… Por ejemplo, hay recientes muestras de secuestros de altos directivos de empresas francesas por parte de los propios empleados.

- Complementar con actividades de inteligencia. Simplemente, se trata de disponer de capacidad para ver y comprender no sólo el perímetro a proteger, sino las interioridades y el entorno próximo y lejano de la entidad en cuestión. Las tareas de inteligencia en ámbito privado y en el público deben regirse por otro ciclo bien conocido, en el que las cuatro fases de planeamiento, obtención de la información, análisis y elaboración de inteligencia, y su posterior difusión constituyen en sí mismas toda una metodología particular. Al igual que la actividad de inteligencia en el ámbito público debe estar en perfecta alineación con los intereses del Estado siguiendo las pautas del gobierno, la inteligencia empresarial debe disponer de un marco de actuación definido y en perfecta sintonía con el negocio. Por otro lado, es imperativa la articulación de un sistema real y eficaz de intercambio de inteligencia entre los ámbitos público y privado. En la actualidad, a pesar de las iniciativas y proclamas oficiales en materia de inteligencia económica en España, nuestras empresas continúan preguntándose cuál es la ventanilla de qué agencia a la que acudir para cubrir su necesidad de inteligencia antes de realizar una operación en el exterior en condiciones de seguridad. Las consultoras complementan el esfuerzo propio, pero la realidad invita a actuar de forma más sinérgica. Las necesidades en materia de seguridad global de las empresas son necesidades de seguridad global para el Estado.[3] Pensemos en la celebración del Bicentenario de las independencias en América Latina que se celebrará en 2010, y en los intereses públicos y privados que están en juego. Y no es una llamada al proteccionismo.

[2] Especificación de requisitos para sistemas de gestión integrada.
[3] Véase J.L. Hernangómez, "Seguridad de la empresa, seguridad del Estado", *Revista Atenea*, nº 4, Madrid, 2009, pp. 62-64.

- Priorizar riesgos. Las metodologías y herramientas habitualmente disponibles realizan la misma operación: cruzar amenazas con activos y determinar un catálogo de riesgos. En este punto es donde quizá se haga más evidente la carencia de una metodología y de una herramienta capaz de realizar este cruce de datos recopilados. Los proveedores de seguridad de alto nivel tienen un gran campo de trabajo en el que demostrar nuevamente su buen hacer profesional y su compromiso por solucionar la necesidad de las empresas que buscan un instrumento con el que realizar sus análisis de riegos convergente y gestionar su seguridad de modo realmente global. El producto de esta fase debe ser una relación de riesgos, ordenados de mayor a menor severidad.

- Determinar el umbral de aceptabilidad. Esta es una cuestión que, con el asesoramiento de los responsables de la gestión de la seguridad y por tanto de los riesgos, debe tomar la dirección de la empresa o, en su caso, del organismo del Estado que corresponda. La decisión de decir qué riesgos son tolerables y admisibles y cuáles no –y que, por tanto, deberán ser gestionados– es de gran trascendencia, pues provocará que unos riesgos sean obviados mientras que otros sean gestionados mediante recursos propios, la transferencia de responsabilidad a terceras partes o por la vía del aseguramiento. Este es uno de los pasos que pone de manifiesto que no hay seguridad sin comunicación, y que el acierto en la transmisión de la información a la dirección es clave a la hora de decidir qué riesgos obviar y a cuáles y en qué orden hacer frente. Tanto la dirección como el gestor de la seguridad, y por tanto del riesgo, deben tener muy presente que la seguridad debe estar alineada con el negocio, que es el negocio el que manda y que la seguridad debe posibilitar ese negocio en condiciones de seguridad. En última instancia, la dirección del negocio es responsable de la seguridad del mismo.

- Elaborar y ejecutar planes y proyectos de implantación de contramedidas. Tomada la decisión acerca de los riesgos a gestionar, deberán desarrollarse los planes de acción correspondientes para implantar las contramedidas necesarias para llevar el nivel de riesgo al valor deseado por la dirección. Esta fase exige disponer de la organización y de los medios adecuados. Obviamente, el compromiso de la dirección es absolutamente clave.

- Asegurar la verificación de la implantación de las contramedidas. Para ello, es necesario que los responsables de seguridad puedan verificar que la exigencia de implantación de contramedidas se ha traducido en su implantación mediante medios propios del departamento de seguridad o la contratación de auditores externos. Ello exige tener la metodología desarrollada, haber definido métricas y disponer de herramientas de monitorización.

- Prever la gestión de crisis. Tanto en el ámbito público como privado, la gestión de crisis debe estar incluida en la gestión de la seguridad global, teniendo creada la orgánica necesaria y dispuestos los recursos humanos y materiales necesarios para responder de forma inmediata y eficiente a una crisis. Las crisis avisan siempre, pero no siempre esos avisos son detectados o atendidos. Si sufrimos crisis es porque nos sorprenden. Si no, hablaríamos de incidentes normales propios del funcionamiento habitual de las empresas y organismos públicos y privados. La gestión de crisis, por tanto, debe estar imbricada con la gestión de riesgos y la seguridad global. Ello debería llevar, por ejemplo, a una mayor integración entre los centros de control de seguridad física o medioambiental o

laboral con los conocidos SOC de seguridad lógica. Las empresas privadas y los organismos públicos que pretendan disponer de una capacidad de gestión de crisis, deberán articular auténticas salas de situación o de crisis, físicas y virtuales, que permitan la continuidad del sistema.

- Disponer de una estrategia y de planes de información y de comunicación. La comunicación es una realidad omnipresente en la gestión del riesgo y de la seguridad. Informar adecuadamente a la audiencia, sea interna o externa a la empresa o institución, es un asunto de vital importancia. La audiencia externa puede ser muy variada, tanto en territorio nacional como, en su caso, extranjero: el gran público, los medios de comunicación, terceras partes como proveedores, competidores, accionistas, clientes, colectivos como contribuyentes, usuarios de sanidad pública, funcionarios…; pero, sin lugar a dudas, la audiencia más complicada es la interna: la dirección de la empresa, los directivos y empleados en general. Es en este campo donde los gestores de los riesgos y de la seguridad global deben emplearse a fondo para formar si no hay formación, convencer si no hay convencimiento, e implicar si no hay implicación.

Conclusiones

Problemas y propuestas

Como conclusiones de esta reflexión, expondremos algunos de los problemas de fondo en la situación actual, así como algunas medidas que contribuirían a modificar el estado de las cosas. En cuanto a los problemas, citaremos:

- Separatismo. Se observa falta de alineación entre el negocio y la seguridad, por parte de ambas esferas; insuficiente convergencia entre las distintas disciplinas de seguridad, como la física, la lógica, la medioambiental, la laboral, la jurídica…; y ausencia o escasez de foros que integren a personas con diferentes responsabilidades en la empresa y en las instituciones. Existen multitud de foros de seguridad que reúnen a convencidos de la seguridad y diversos foros de negocios que reúnen a convencidos del negocio, pero es difícil encontrar foros donde trabajen simultáneamente implicados en operaciones de negocio y en la gestión de la seguridad. Todo ello genera inseguridad. Es preciso disponer de puntos de encuentro para empresarios y gestores de la seguridad de sus negocios, donde de forma sinérgica se expongan problemas, necesidades y soluciones aceptables y con el compromiso de cuantos se han de sentir en el mismo barco.

- Estereotipos. Hay que lograr que los hombres del negocio entiendan y no se desentiendan de los riesgos de seguridad, de los que son responsables; que los gestores de riesgos y seguridad comprendan la importancia de la cuenta de resultados; y que todos asuman que el negocio realmente incluye tanto las tareas “propias” (comerciales, financieras, de recursos humanos…) como las de seguridad. Todas forman parte indisociable del mismo juego. Esto es aplicable, por descontado, al Estado y a sus instituciones, así como a sus múltiples activos. Valga un símil: el coche de Fernando Alonso necesita mucho motor, pero también medidas de seguridad para poder competir bien y ganar. Sin seguridad, Fernando Alonso no competiría. Existen otros estereotipos que distorsionan el buen funcionamiento de los negocios; por ejemplo, la idiosincrasia de cada empresa o del gobierno de turno, que puede inducir un equivocado enfrentamiento

conceptual entre seguridad-represión por un lado, y progreso-libertad por otro. La seguridad contribuye a la libertad, y la libertad aporta seguridad.

- Agregación de funciones. Es muy peligroso no segregar las funciones implicadas en la marcha diaria de los procesos y sistemas, de aquellas encargadas de vigilar las condiciones de seguridad en las que se desenvuelven las primeras. Esto se ve con claridad en el ámbito TIC, en aquellos casos en los que los responsables del funcionamiento de los sistemas son también responsables de la gestión de los riesgos y de la seguridad. No se puede ser juez y parte, como el auditado no puede ser su auditor. Los gestores de riesgos y de la seguridad deben ser orgánicamente independientes de las demás funcionalidades de la entidad pública o privada.

- Escasez de recursos. Que sea un tópico no resta un ápice de su valor: se necesitan recursos adecuados para la gestión del riesgo y de la seguridad si se quieren resultados acordes con el nivel de seguridad marcado por la dirección. En caso contrario, la dirección deberá asumir un mayor riesgo y su responsabilidad correspondiente. Por supuesto, la gestión de riesgos y de seguridad incurre en gastos, pero tanto los responsables de dicha gestión como la dirección última del negocio o del Estado deben aceptar como incuestionable que, dentro de los márgenes razonables de las actuaciones razonables, los desembolsos en seguridad constituyen una inversión con un retorno claro: la evitación o la mitigación de riesgos contribuye de forma matemática a la evitación o reducción de pérdidas, en ocasiones muy severas y de difícil de cuantificación. En todo caso, los gestores del riesgo y de la seguridad, como cualquier otro departamento perteneciente al engranaje global, están subordinados a las decisiones; pero no es menos cierto que también la alta dirección asume automáticamente la responsabilidad de la merma en seguridad. Este asunto es especialmente delicado en tiempos de crisis como el actual y flaco favor se hace al estado general de las cosas si en tiempos de riesgos elevados y crecientes no se adecúan en la proporción debida los mecanismos de protección.

- Vacío metodológico e instrumental. Debemos desarrollar metodologías y herramientas estandarizadas y globales que permitan realizar análisis de riesgos de una forma convergente y global. Ya hay empresas privadas que, con el apoyo de consultoras especializadas, han desarrollado aproximaciones a dicha convergencia mediante la generación de un sistema de gestión de la seguridad corporativa que integre las disciplinas de seguridad necesarias, inteligencia incluida.

Frente a este catálogo de problemas relacionados con las metodologías y la gestión del riesgo y de la seguridad, pensamos que hay medidas, no exentas de complejidad, que contribuirían a cubrir las carencias existentes y a corregir las desviaciones observadas. Estas medidas deberían provocar:

- Mayor integración entre responsables de seguridad y del resto de áreas de negocio –entre proveedores de seguridad y consumidores de seguridad, tanto del ámbito público como del privado– y dentro de una misma empresa o institución, tanto en aspectos orgánicos como en procedimentales.

- Mayor esfuerzo normativo, a fin de lograr unos estándares aceptables e incluso certificables en la gestión del riesgo y de la seguridad global.

- Mayor intensidad en investigación, para desarrollar herramientas que posibiliten la implantación de metodologías y la gestión del riesgo de forma convergente.

- Mayor intensidad en la comunicación entre las diferentes audiencias interna y externa.

- Suficiente dotación de medios para el desarrollo e implantación de metodologías, análisis y sistemas de gestión del riesgo y de la seguridad.

- Crear una sinergia real en el ámbito de la inteligencia entre Estado y empresas, superando el "efecto esponja" que parece presidir unas relaciones en las que el Estado se apoya en las empresas y éstas no se benefician de un retorno adaptado a sus necesidades.

Saltar de las musas al teatro no es fácil, pero es preciso, máxime en los tiempos actuales, articular medidas reales y efectivas que permitan ofrecer respuestas de seguridad global a la globalidad de los riesgos a los que nos enfrentamos. Utilicemos las sinergias posibles entre lo público y lo privado, provengan de los negocios, de las universidades, de los *think tanks* o de particulares, y demos un paso adelante más allá de las retóricas. La esfera privada y la pública gozan de espacios propios pero también de un espacio común, tienen responsabilidades particulares y también colectivas. La gestión del riesgo público y privado en ocasiones se diferencia solamente en que éste no dispone de fondos reservados, pero no siempre necesarios. Estos últimos tiempos, todos hemos podido constatar ejemplos dramáticos de lo difusa que llega a ser la frontera entre el interés público y el privado. Actuemos en consecuencia.

José Luis Hernangómez de Mateo
Director de Planificación y Alertas del Grupo Prisa, doctor en Ciencias Políticas y Sociología, coronel en situación de reserva, especialista en Investigación Operativa, director de Seguridad y auditor SGSI, con una acreditada experiencia en inteligencia